

PARADIGM *Research*

PUBLIC FORUM **Position Paper**



NOVEMBER
2013-2014

**THE BENEFITS OF DOMESTIC SURVEILLANCE
BY THE NSA OUTWEIGH THE HARMS.**

If you enjoyed this fine book from PARADIGM RESEARCH,
you'll be glad to know that we offer a complete menu
of affirmatives, disadvantages, counterplans, kritiks,
LD & Public Forum research, and much more.

Shop our online store anytime - www.oneparadigm.com

Call us for a free catalog toll-free - 800-837-9973

The Paradigm NFL Public Forum Position Paper
November 2013
by Dr. David Cram Helwich

Copyright © 2013 by Paradigm Research, Inc. All rights reserved.

First Edition Printed In The United States Of America

For information on Paradigm Debate Products:

PARADIGM RESEARCH

P.O. Box 2095

Denton, Texas 76202

Toll-Free 800-837-9973

Fax 940-380-1129

Web /www.oneparadigm.com/

E-mail service@oneparadigm.com

All rights are reserved. This book, or parts thereof, may not be reproduced by any means - graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems - without the written permission of the publisher. Making copies of this book, or any portion, is a violation of United States and international copyright laws.

NSA Surveillance: Table of Contents

NSA Surveillance: Overview.....	3
---------------------------------	---

NSA Surveillance Desirable

Surveillance Desirable: Topshelf.....	8
Surveillance Desirable: Public Supports / Accepts	11
Surveillance Desirable: Terror—Topshelf	14
Surveillance Desirable: Terror—Allies	15
Surveillance Desirable: Terror—Bush Era Programs	16
Surveillance Desirable: Terror—Empirically True	17
Surveillance Desirable: Terror—Key to Prevention	20
Surveillance Desirable: Terror—Metadata-Specific	23
Surveillance Desirable: Terror—Presidential Flexibility Key	28
Surveillance Desirable: Terror—PRISM-Specific	29
Surveillance Desirable: Terror Threat—Al Qaeda	30
Surveillance Desirable: Terror Threat—Bioterrorism	33
Surveillance Desirable: Terror Threat—Nuclear Terrorism	34
Surveillance Desirable: Terror Threat—Answers to “Bioterror Unlikely”	35
Surveillance Desirable: Terror Threat—Answers to “Bin Laden Death Solves Threat”	36
Surveillance Desirable: Terror Threat—Answers to “Border Security”	37
Surveillance Desirable: Terror Threat—Answers to “Nuclear Materials Unavailable”	38
Surveillance Desirable: Terror Threat—Answers to “Nuclear Threat Exaggerated”	39
Surveillance Desirable: Terror Threat—Answers to “Won’t Go Nuclear” (General)	40
Surveillance Desirable: Terror Threat—Answers to “Won’t Go Nuclear” (Al Qaeda)	41
Surveillance Desirable: Answers to “Chilling Effect”	43
Surveillance Desirable: Answers to “Illegal / Overreach”	44
Surveillance Desirable: Answers to “Privacy”—Citizen Surveillance	46
Surveillance Desirable: Answers to “Privacy”—Dead	47
Surveillance Desirable: Answers to “Privacy”—Fourth Amendment	49
Surveillance Desirable: Answers to “Privacy”—General	51
Surveillance Desirable: Answers to “Privacy”—Internal Safeguards	54
Surveillance Desirable: Answers to “Privacy”—Metadata	56
Surveillance Desirable: Answers to “Privacy”—Minimal Intrusion	57
Surveillance Desirable: Answers to “Privacy”—Other Invasions Worse	58
Surveillance Desirable: Answers to “Privacy”—Oversight Solves	59
Surveillance Desirable: Answers to “Privacy”—Section 215-Specific	61
Surveillance Desirable: Answers to “Privacy”—Section 702-Specific	62

NSA Surveillance Undesirable

Surveillance Undesirable: Topshelf.....	63
Surveillance Undesirable: Chilling Effect.....	67
Surveillance Undesirable: Cybersecurity	69
Surveillance Undesirable: Democracy	70
Surveillance Undesirable: Economic Effects	72
Surveillance Undesirable: International Backlash—Europe	76
Surveillance Undesirable: International Backlash—Latin America	78
Surveillance Undesirable: International Law	79
Surveillance Undesirable: Privacy—General	82
Surveillance Undesirable: Privacy—Monitoring of Innocents	84
Surveillance Undesirable: Privacy—Section 215 / Metadata	86
Surveillance Undesirable: Privacy—Section 702 / PRISM	89
Surveillance Undesirable: Privacy—Answers to “Citizens Exempted”	91
Surveillance Undesirable: Privacy—Answers to “Info Not Shared”	94
Surveillance Undesirable: Privacy—Answers to “Intel Only”	95
Surveillance Undesirable: Privacy—Answers to “Internal Safeguards”	96
Surveillance Undesirable: Privacy—Answers to “Limited Data Timeframe”	99
Surveillance Undesirable: Privacy—Answers to “Metadata Ignores Content”	101
Surveillance Undesirable: Privacy—Answers to “Minimal Intrusion”	104
Surveillance Undesirable: Privacy—Answers to “Not Domestic”	105
Surveillance Undesirable: Privacy—Answers to “Oversight—FISA Court”	107
Surveillance Undesirable: Privacy—Answers to “Oversight—General”	111
Surveillance Undesirable: Privacy—Answers to “Social Networks Exempted”	113
Surveillance Undesirable: Answers to “Terrorism”—Topshelf.....	114
Surveillance Undesirable: Answers to “Terrorism”—Biological	115
Surveillance Undesirable: Answers to “Terrorism”—Effectiveness Exaggerated	116
Surveillance Undesirable: Answers to “Terrorism”—Info Overload	118
Surveillance Undesirable: Answers to “Terrorism”—Nuclear	119

NSA Surveillance: Overview

Resolved: The benefits of domestic surveillance by the NSA outweigh the harms.

Piggybacking on an older, Bush-era controversy that gained renewed political prominence with the revelations by leaker Edward Snowden this past June, the November NFL Public Forum resolution tasks students with assessing the merits of domestic surveillance programs conducted by the National Security Administration (NSA), the federal agency (established in 1952) that has primary responsibility for electronic intelligence gathering. This topic seems to be pretty well balanced and revisits many of the “security versus freedom” questions that have informed post-9/11 public policymaking and debating alike. This essay includes an overview the latest political controversy over NSA domestic surveillance programs and an assessment of some of the strongest pro and con arguments on the topic.

Public and private debates over the desirability of domestic surveillance (or “spying”, if one wants to avoid the use of unnecessary euphemism) are nearly as old as the republic. Fear of the invasiveness of British law enforcement and military action played a role in inspiring the American Revolution, and very strong protections against undue government surveillance are written into the nation’s founding documents, particularly the Fourth Amendment, which states:

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

These words have been interpreted by the courts and legal historians both as offering protection against warrantless searches and seizures, and have also served as the basis for an emerging right to privacy. Interpretations of the meaning and scope of the Fourth Amendment have become increasingly complicated by the development and widespread adoption of new communications technologies. Such technologies (everything from telegraphs to cell phones to the internet) make it much easier for individuals to communicate with one another, but they also raise legitimate concerns about the possibility that government agents and even private actors can “tap in” on such communications, compromising individual privacy rights. For the most part, the federal judiciary has held that protections afforded to a person’s “papers” also apply to most forms of electronic communication, although these rights tend to be balanced against the interests of the state in promoting public order and protecting the nation against armed attack. There has been a constant battle between forces advocating stronger privacy protections and actors who claim that the emergence of “new” threats and technologies require a rethinking of “eighteenth century” notions of privacy. Although these disputes obviously resonate strongly in a post 9/11 context, such arguments have been ongoing for many decades, as evidenced by controversies surrounding the surveillance of suspected communists during the Cold War and activities of the federal government directed towards leaders of the civil rights movement. Questions of the gathering of “foreign intelligence” and how such intersect with private, domestic communications have been particularly troublesome, leading to the passage of the Foreign Intelligence Surveillance Act (FISA) in the late 1970s, which imposed restrictions on domestic spying activities and created a special FISA Court to rule on government requests to engage in domestic surveillance relating to ongoing intelligence investigations. Many of the concerns surrounding the original FISA are evident in today’s debates about the scope and desirability of the NSA’s surveillance programs. The issues raised by this topic are thus at the heart of an important and ongoing moral and political controversy that dates to our nation’s earliest days.

The current topic is likely inspired by the recent revelations of massive surveillance programs conducted by the NSA. These programs were well-known to select members of congress and authorities within the executive branch, but only became widespread public knowledge as the result of a series of leaks by Edward Snowden, a former contractor with the NSA who collected and disseminated evidence of large-scale government surveillance programs. These programs were first reported publicly in *The Guardian* and *Washington Post* on June 6, 2013. Snowden’s leaks re-ignited a controversy dating back to the George W. Bush administration, when it was revealed that government agencies had been authorized to engage in widespread surveillance of communications between U.S. citizens and persons outside of the United States. A recent report from the Congressional Research Service (CRS) summarizes the current controversy:

Recent media stories about National Security Agency (NSA) surveillance address unauthorized disclosures of two different intelligence collection programs. These programs arise from provisions of the Foreign Intelligence Surveillance Act (FISA). However, they rely on separate authorities, collect different types of information, and raise different policy questions. As such, where possible, the information contained in this report distinguishes between the two. For both programs, there is a tension between the speed and convenience with which the government can access data of possible intelligence value and the mechanisms intended to safeguard civil liberties. The first program collects and stores in bulk domestic phone records that some argue could be gathered to equal effect through more focused records requests. The

NSA Surveillance: Overview [cont'd]

second program targets the electronic communications of non-U.S. citizens but may incidentally collect information about Americans. [Marshall Curtis Erwin, and Edward C. Liu, Congressional Research Service, “NSA Surveillance Leaks: Background and Issues for Congress,” CRS REPORT FOR CONGRESS, 7—2—13, p. 1]

The metadata program has been justified under Section 215 of the PATRIOT Act, first passed after the 9/11 attacks and subsequently re-authorized by congress. The CRS provides a succinct assessment of the Section 215 provisions:

Section 215 of the USA PATRIOT ACT, which is the authority cited by the DNI as the basis of the recently revealed collection of domestic phone records, broadened government access by both enlarging the scope of materials that may be sought and lowering the legal standard required to be met. Specifically, Section 215 modified the business records provisions of FISA to allow the FBI to apply to the FISC for an order compelling a person to produce “any tangible thing,” including records held by a telecommunications provider concerning the number and length of communications, but not the contents of those communications. In 2005, the provision was further amended to require the FBI to provide a statement of facts showing that there are “reasonable grounds to believe” that the tangible things sought are “relevant to an authorized investigation (other than a threat assessment)” into foreign intelligence, international terrorism, or espionage. The statute considers records presumptively relevant if they pertain to: • A foreign power or an agent of a foreign power; • The activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or • An individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation. The phrase “reasonable grounds to believe” is not defined by FISA, but has been used interchangeably with the “reasonable suspicion” standard, a less stringent standard than “probable cause.” Although there are not any publicly available judicial opinions interpreting this language in the context of Section 215, it may be helpful to look at appellate courts’ interpretations of the Stored Communications Act (SCA), as it similarly authorizes law enforcement to access telecommunications transactional records (as well as stored electronic communications) upon a showing that “there are reasonable grounds to believe” that the information sought is “relevant and material to an ongoing criminal investigation.” Under the SCA, the collection of stored email has been held to meet that standard in the context of a “complex, large-scale mail and wire fraud operation” in which “interviews of current and former employees of the target company suggest that electronic mail is a vital communication tool that has been used to perpetuate the fraudulent conduct” and “various sources [have verified] that [the provider who had custody of the email] provides electronic communications services to certain individual(s) [under] investigation.” Similarly, obtaining the internet protocol (IP) address and name associated with a Yahoo! account was justified when a police officer received a tip from an individual that he had received what appeared to be child pornography from that Yahoo! account. [Marshall Curtis Erwin, and Edward C. Liu, Congressional Research Service, “NSA Surveillance Leaks: Background and Issues for Congress,” CRS REPORT FOR CONGRESS, 7—2—13, p. 4-5]

The metadata program is controversial primarily because it includes the collection of massive volumes of phone records of U.S. citizens, something that many critics have labeled as illegal domestic surveillance. The CRS report includes an assessment of many of the major components of the alleged ‘scandal’:

Domestic Collection of Domestic Phone Records—collected under Section 215 of the USA PATRIOT ACT: On Wednesday, June 5, 2013, The Guardian reported that NSA collects in bulk the telephone records of millions of U.S. customers of Verizon Wireless, pursuant to an order from the Foreign Intelligence Surveillance Court (FISC). Intelligence officials and leaders of the congressional intelligence committees have confirmed the existence of this domestic phone records collection program, although they have not identified the companies providing the records. It has been alleged but not confirmed that similar orders have been sent to other telecommunications providers. The court order disclosed by The Guardian was a three-month extension of a program that has been going on for seven years. The Director of National Intelligence (DNI) has acknowledged the breadth of the program, analogizing it to “a huge library with literally millions of volumes of books,” but has stated that data about Americans in the possession of the United States government can only be accessed under specific circumstances. The program collects “metadata”—a term used in this context to refer to data about a phone call but not the phone conversation itself. Intelligence officials have stated that the data are limited to the number that was dialed from, the number that was dialed to, and the date and duration of the call. The data must be destroyed within five years of acquisition. Information collected does not include the location of the call (beyond the area code identified in the phone number), the content of the call, or the identity of the subscriber. However, some civil liberties advocates have argued that a telephone number today is essentially a unique identifier that can be easily tied to a person’s identity by other means and that the distinction between a telephone number and subscriber identity is therefore insignificant. On June 27, 2013, The Guardian published an article alleging that NSA previously collected the metadata for Internet-based communications (email being the prime example) for Americans

NSA Surveillance: Overview [cont'd]

inside the United States. A spokesman for the DNI confirmed The Guardian's account but said this program was discontinued in 2011. Intelligence officials have stated that, pursuant to the same FISA authorities, NSA does not currently collect in bulk the metadata of these types of communications. It has been suggested that this type of collection was also conducted pursuant to the same FISA Section 215 authorities, and some have expressed concern that those authorities could again be used to collect Internet metadata in the future. [Marshall Curtis Erwin, and Edward C. Liu, Congressional Research Service, "NSA Surveillance Leaks: Background and Issues for Congress," CRS REPORT FOR CONGRESS, 7—2—13, p. 1-2]

The second component of the controversy concerns the NSA's gathering of content-focused data of citizens who communicate with "suspects" overseas. These activities are authorized under a series of amendments to FISA that were implemented in 2008, particularly Section 702, which is outlined by the CRS:

Foreign Internet-Related Data: Title VII, added by the FISA Amendments Act of 2008, provides additional procedures for the acquisition of foreign intelligence information regarding persons who are believed to be outside of the United States. The DNI has stated that the recently disclosed collection of foreign intelligence information from electronic communication service providers has been authorized under Section 702 of FISA, which specifically concerns acquisitions targeting non-U.S. persons who are overseas. Prior to the enactment of Section 702, and its predecessor in the Protect America Act of 2007, FISA only authorized sustained electronic surveillance or access to electronically stored communications after the issuance of a FISC order that was specific to the target. The FISC, in authorizing electronic surveillance or a physical search, must find probable cause to believe both (1) that the person targeted by the order is a foreign power or its agent, and (2) that the subject of the search (i.e., the telecommunications or place to be searched) is owned, possessed, or will be used by the target. Section 702 permits the Attorney General (AG) and the DNI to jointly authorize targeting of persons reasonably believed to be located outside the United States, but is limited to targeting non-U.S. persons. Once authorized, such acquisitions may last for periods of up to one year. Under subsection 702(b) of FISA, such an acquisition is also subject to several limitations. Specifically, an acquisition: • May not intentionally target any person known at the time of acquisition to be located in the United States; • May not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States; • May not intentionally target a U.S. person reasonably believed to be located outside the United States; • May not intentionally acquire any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States; and • Must be conducted in a manner consistent with the Fourth Amendment to the Constitution of the United States. Acquisitions under Section 702 are also geared towards electronic communications or electronically stored information. This is because the certification supporting the acquisition, discussed in the next section, requires the AG and DNI to attest that, among other things, the acquisition involves obtaining information from or with the assistance of an electronic communication service provider. This would appear to encompass acquisitions using methods such as wiretaps or intercepting digital communications, but may also include accessing stored communications or other data. Central components of Section 702 are the targeting and minimization procedures that must be submitted to the FISC for approval. In order to be approved, Section 702 requires the targeting procedures be reasonably designed to ensure that an acquisition is limited to targeting persons reasonably believed to be located outside the United States, and to prevent the intentional acquisition of any communication where the sender and all intended recipients are known at the time of the acquisition to be located in the United States. [Marshall Curtis Erwin, and Edward C. Liu, Congressional Research Service, "NSA Surveillance Leaks: Background and Issues for Congress," CRS REPORT FOR CONGRESS, 7—2—13, p. 6-7]

Leaks about the program spurred a proverbial 'political firestorm,' since PRISM seems to contravene previous government statements that its surveillance schemes do not review the content of the communications of American citizens without a warrant from the FISA Court:

Domestic Collection of Foreign Internet-Related Data—collected under Section 702 of FISA: The Washington Post reported on June 6th, 2013, that, "The National Security Agency and the FBI are tapping directly into the central servers of nine leading U.S. Internet companies, extracting audio and video chats, photographs, e-mails, documents, and connection logs that enable analysts to track foreign targets." The Guardian ran a similar story that same day. These articles referred to a system called PRISM allegedly used to collect this data. Outside commentators and government officials have argued that portions of these stories are inaccurate. Public comments from the Administration indicate this intelligence collection is more targeted in scope than was suggested by these articles, and major technology companies have denied giving the federal government direct access to their servers. The DNI on June 8, 2013, released a public

NSA Surveillance: Overview [cont'd]

statement saying, “The Guardian and Washington Post articles refer to collection of communications pursuant to Section 702 of the Foreign Intelligence Surveillance Act.” A fact sheet provided by the DNI stated that PRISM is an internal government computer system used to facilitate access to these communications. In accordance with Section 702, this collection program appears largely to involve the collection of data, including the content of communications, of foreign targets overseas whose emails and other forms of electronic communication flow through networks in the United States. Compared to the breadth of phone records collection under Section 215, this program is more discriminating in terms of its targets but broader in terms of the type of information collected. Beyond that, the scope of the intelligence collection, the type of information collected and companies involved, and the way in which it is collected remain unclear. Examples cited by the Administration include the email content of communications with individuals inside the United States, but in those cases the targets of the intelligence collection appear to have been non-U.S. citizens located outside the United States. On June 20, 2013, The Guardian also published NSA’s targeting and minimization procedures for information collected under Section 702 authorities. Documents referred to in the article specify the procedures used to determine that the targets of intelligence collection are non-U.S. persons located outside the United States and the procedures used to minimize the retention and dissemination of information about U.S. persons collected under Section 702 authorities. [Marshall Curtis Erwin, and Edward C. Liu, Congressional Research Service, “NSA Surveillance Leaks: Background and Issues for Congress,” CRS REPORT FOR CONGRESS, 7—2—13, p. 2-3]

The programs are also controversial because they targeted many nations and organizations, including terrorist groups (like Al Qaeda), states with sometimes conflictual relations with the U.S. (such as China, Iran, and Russia), and even American allies.

For its part, the National Security Administration has provided a defense of the legality and necessity of both of these programs. The NSA documents and the Snowden leaks show that the programs are targeted at enhancing American counter-terrorism capabilities, the assessment of the stability of other countries, and the gathering of commercial secrets. An official document outlining the NSA arguments can be found here:

<<http://www.nsa.gov/public_info/_files/speeches_testimonies/2013_08_09_the_nsa_story.pdf>>

The resolution suggests a simple cost-benefit analysis. Impact assessment will be vital. You should also be careful to center your arguments on both sides of the resolution on *domestic* surveillance, although the broad nature of the NSA’s data gathering and analysis schemes means that they all have a domestic element. Pro cases should focus on emphasizing the deadly nature of the terrorist threat facing the United States. Although the death of Osama bin Laden and other leaders demonstrate the considerable progress that the nation is making in its war against Al Qaeda and other organizations targeting the U.S., there is very strong evidence indicating that Al Qaeda and other groups remain dangerous. In particular, Al Qaeda affiliate groups, such as various organizations operating in Afghanistan and Pakistan, AQAP (Al Qaeda in the Arab Peninsula, predominately operating in Yemen and surrounding areas) and AQIM (Al Qaeda in the Islamic Maghreb, based in North Africa) have become increasingly well organized and aggressive in their efforts to undermine U.S. interests in Southwest Asia, the Middle East and North Africa. Such organizations threaten the stability of vital governments in the region (such as Pakistan, Saudi Arabia, Bahrain, and Libya), target U.S. military facilities, and are actively engaged in subverting vital U.S. foreign policy initiatives. The oft-cited “nightmare scenario” is that such an organization buys, steals, or constructs a nuclear weapon, which is could then use to coerce massive concessions from Western governments, to destroy a major Western city, or to spark a (miscalculated) inter-state war that carries its own escalation risks. There is also strong evidence that the emergence of new biotechnologies also presents the risk of a successful terrorist attack with biological weapons (bioterror), which could have horrific consequences. Defenders of the NSA programs argue that surveillance (including the criticized domestic elements of those programs) have foiled literally dozens of ripe terrorist plots, and that the intelligence information obtained from such programs are vital in disrupting terrorist networks and directing the targeted killing (drone) missions that have decimated the leadership of Al Qaeda and other organizations. The oft-criticized metadata analysis programs are particularly important, since they allow intelligence analysts to discern communication patterns that reveal clandestine terrorist activities that would otherwise escape scrutiny. The pro side also has a number of strong arguments defending against the “civil rights” and “privacy” claims that will serve as the centerpiece of con cases. First, external oversight, including the need to seek consent from the FISA Court, helps ensure that any data collected is directly linked to terrorist investigations. Congress also has the authority to oversee and guide the NSA programs, both deterring potential abuse and providing an important procedural safeguard, since Congress can simply alter the program protocols if they raise serious constitutional concerns. The NSA has also adopted a number of internal safeguards that make it difficult to link information to specific persons and will prevent other entities from obtaining access to information about citizens’ communications without a warrant. There is very good evidence defending both the Section 215 and Section 702 programs. Furthermore, the concept of privacy defended in most con evidence is seriously outdated and does not reflect the realities of

NSA Surveillance: Overview [cont'd]

an increasingly networked world. Other entities outside of government, especially private businesses (such as Google and Facebook), engage in far more invasive datamining than does the NSA. Domestic monitoring by the NSA is only a very small, but critical, part of surveillance programs that have been vital in preventing further terrorist attacks against the United States. There is an evitable tradeoff between privacy and security, and polling indicates that the American public is quite willing to accept a small risk of minor privacy invasions in exchange for securing the homeland. Finally, any concerns about the program will likely be addressed by looming congressional and executive branch oversight reforms, demonstrating both the resiliency of our political system and the strong capacity of our government to minimize rights infringements in the ongoing fight against Al Qaeda.

You should consider focusing your con cases on two general argument categories. First, you should attack the pro claim that PRISM et al. are effective and necessary in preventing terrorist attacks. Although the NSA Director and other program defenders have argued that the programs are directly responsible for stopping over 50 terrorist attacks, subsequent investigation calls these claims into question, with some analysts maintaining that very few, or perhaps no, attacks have been directly stopped by NSA surveillance. There is also considerable reason to believe that other intelligence methods are more effective in preventing terrorist attacks, with some NSA critics contending that the NSA schemes will only catch the inept terrorist groups that would end up being apprehended through any number of other channels. Some evidence indicates that most “terror traffic” occurs on portions of the internet that are highly resistant to NSA surveillance, and that Al Qaeda and other organizations avoid the parts of the web that are targeted by the NSA’s “dragnet” operations. The NSA program’s reliance on massive volumes of data may also make it more difficult to detect terrorist activity by overloading the human and electronic analytic capacities of the agency. The pro case is also vulnerable to claims that the threat posed by terrorist groups are largely exaggerated—analysts have been fearful of a nuclear or biological terrorist attack for decades, yet no such attack has occurred. The con side has access to excellent evidence which argues that terrorist groups tend to avoid using nuclear and/or biological weapons because they do not serve the organization’s interests, because they are very difficult to use, and because of the threat of a massive international backlash in the face of a successful strike. Second, con teams need to emphasize the very real threat to civil rights posed by PRISM, XKeyscore, Tempora, etc. Critics contend that the NSA’s claims that metadata analysis ignores the activities of specific internet and cellphone users are disingenuous, with highly-qualified sources arguing that such data can be used to draw very accurate individual profiles. The fact that the NSA stores individual user data, oftentimes for years in case such data will be needed in a future, warrant-driven investigation, raises serious privacy risks for individuals from the NSA, other government agencies which may obtain access to such data, and from outside groups that could hack into the NSA databases. Perhaps even more importantly, the looming specter of potential surveillance has a profound “chilling effect,” instilling fear in citizens who end up curtailing their legitimate internet/communications activities because they are afraid that such activities will be monitored by government agents or revealed at some future date. The expectation of privacy allows people to freely share their thoughts and ideas with others without fear of government recrimination or public denouncement, and such free communication is the foundation of dissent and democratic governance. Con teams also have access to arguments about how the NSA programs have sparked a strong backlash from other governments, who have threatened to curtail cooperation (including in the counterterrorism realm) with the United States. U.S. tech companies are also facing a much more hostile marketplace, with many potential international clients threatening to avoid doing business with American companies that they believe may be forced to turn over valuable data to the U.S. government.

Best of luck!

Surveillance Desirable: Topshelf

1. Only NSA-style surveillance can address the new terrorist threats

Michael Chertoff, former Director, Homeland Security, "NSA Surveillance Vital to Our Safety," USA TODAY, 9—11—13, www.usatoday.com/story/opinion/2013/09/11/nsa-privacy-chertoff-911-column/2793063/, accessed 10-4-13.

In the aftermath of September 11, 2001, the intelligence community was criticized for failing to "connect the dots." Our investigation of the attack revealed connections among the 9/11 hijackers themselves as well as communications they had with known foreign terrorist locations overseas. One example discovered was that of communication between 9/11 hijacker Khalid al-Mihdhar who was in California and a known al-Qaeda safe house in Yemen. At the time, the National Security Agency had collected the Yemen end of the communications. However, due to the nature of this collection, the U.S. government had no way of determining the telephone number or the location of al-Mihdhar. Had the government been able to locate him in San Diego, it might well have been the key lead to disrupting the 9/11 attacks. This type of signals intelligence – the ability to intercept signals or communications particularly where there is a reason to believe one or more parties is a foreign terrorist -- is essential in today's modern world of global networks and interaction. It is with this in mind and the vivid memory of 9/11 that the intelligence community and in particular, the National Security Agency, has developed new counterterrorism capabilities that allow us to better detect and pinpoint terrorist threats to the U.S. It is exactly these types of capabilities, authorized repeatedly by Congress and the Foreign Intelligence Surveillance Court, and with strict legal oversight by the Department of Justice and the Office of the Director of National Intelligence, which allowed us to hunt down terrorists overseas and disrupt dozens of harmful plots since 9/11. I have described intelligence today as equivalent to the 21st Century version of radar. Previously, when the U.S. feared an attack, we used radar as our eyes and ears to detect enemy aircraft or bombs that may be heading for the U.S. or Europe. However, this is not possible when dealing with terrorists who operate in often remote, ungoverned places around the world with no traditional weapons or military fleets. This enemy is different. They disguise themselves as civilians and exploit our very own transportation infrastructure and communication networks against us. Terrorists come in under the cover of deception. They cannot be detected by radar. They can only be detected by the use, analysis and sharing of intelligence that allows us to separate those who are a threat from those who are innocent. Often this is accomplished by intercepting information reflecting the communication, financial and travel activity which terrorists must use to plan and execute attacks. This is exactly what the NSA and indeed our entire intelligence community does.

2. We must not hinder the President's power to gather intelligence and protect us from our enemies

John Yoo, visiting scholar, American Enterprise Institute, "Why We Endorsed Warrantless Wiretaps," WALL STREET JOURNAL, 7—16—09, <http://aei.org/article/foreign-and-defense-policy/defense/why-we-endorsed-warrantless-wiretaps/>, accessed 10-3-13.

Every federal appeals court to address the question has agreed that the president may gather electronic intelligence to protect against foreign threats. This includes the special FISA appeals court, which in a 2002 sealed case upholding the constitutionality of the Patriot Act held that "the President did have inherent authority to conduct warrantless searches to obtain foreign intelligence information." The court said it took the president's power "for granted," observing that "FISA could not encroach on the President's constitutional power." Now, according to the inspectors general, those of us in government following the 9/11 terrorist attacks should have assumed that the usual peacetime rules for domestic wiretaps applied and interpreted FISA in a most curious way--to delete the president's traditional authority as commander in chief to collect signals intelligence in wartime. The 1952 Supreme Court case of *Youngstown Sheet & Tube v. Sawyer* is the IG's lodestar. In *Youngstown*, the Court addressed President Harry Truman's effort to seize steel mills shut down by a labor strike during the Korean War. Truman claimed that maintaining production was necessary to supply munitions and material to American troops in combat. *Youngstown* correctly found that the Constitution gives Congress, not the president, the exclusive power to make law concerning labor disputes. It does not, however, address the scope of the president's power involving military strategy or tactics in war. If anything, it supports the proposition that one branch cannot intrude on the clear constitutional turf of another. Moreover, earlier Justice Departments--reaching across several administrations from both parties--had likewise concluded that *Youngstown* did not limit the president's legitimate conduct of foreign affairs and national security policy. This is why all administrations have refused to accept the 1973 War Powers Resolution and have regularly engaged in military conflicts without congressional approval. Our Constitution created a presidency whose function is to protect the nation from attack. Gathering intelligence--including intercepting enemy communications--has long been a key aspect of war. Our military and intelligence agencies cannot attack or defend the nation unless they know where to aim. As we confront terrorists who remain intent on attacking the U.S., using weapons we cannot anticipate, we should be skeptical of those who insist that we radically change the way this country has always made war.

Surveillance Desirable: Topshelf [cont'd]

3. NSA programs are not subject to abuse—multiple reasons

William Saletan, “Stop Freaking out about the NSA,” SLATE, 6—6—13, www.slate.com/articles/news_and_politics/frame_game/2013/06/stop_the_nsa_surveillance_hysteria_the_government_s_scrutiny_of_verizon.html, accessed 10-12-13.

But the program is also restrained in several ways. Here’s a list. 1. It isn’t wiretapping. The order authorizes the transfer of “telephony metadata” such as the date and length of each call and which phone numbers were involved. It doesn’t include the content of calls—which is more tightly protected by the Fourth Amendment—or the identity of the callers. The targeted data are mathematical, not verbal. They’re the kind of information you’d request if you were mapping possible extensions of a terrorist or criminal network. 2. It’s judicially supervised. The leaked document is a court order. It was issued by the Foreign Intelligence Surveillance [FISA] Court. To get the Verizon data, the FBI had to ask the court for permission. The Bush administration used to extract this kind of metadata unilaterally. The Obama administration has changed the rules to bring in the court as an overseer. 3. It’s congressionally supervised. Any senator who’s expressing shock about the program is a liar or a fool. The Senate Intelligence and Judiciary Committees have been briefed on it many times. Committee members have had access to the relevant FISA court orders and opinions. The intelligence committee has also informed all senators in writing about the program, twice, with invitations to review classified documents about it prior to reauthorization. If they didn’t know about it, they weren’t paying attention. 4. It expires quickly unless it’s reauthorized. The leaked order was issued on April 25 and expires on July 19. That’s the way these orders have worked for years: The court has to review and reapprove the surveillance request, or the authority to transfer the records expires. 5. Wiretaps would require further court orders. The reason the leaked order is so broad is that it applies only to metadata. If, after looking at its map of phone numbers, the government decides that yours might belong to a potential terrorist, it can seek further information, including the content of your calls. But in that case, it has to ask the court for a separate order, which in turn would require enough evidence to override your Fourth Amendment rights. Is government surveillance worth worrying about? Sure. But even broad surveillance, per se, isn’t outrageous. What’s important is that the surveillance be warranted by real threats, appropriately limited, and supervised by competing branches of government. In this case, those standards have been met.

4. Minor abuses are inevitable, and we have to accept them as part of having a government that can both govern and protect us—there are no viable alternatives

Eric Posner, Professor, Law, University of Chicago, “Secrecy and Freedom,” NEW YORK TIMES, Room for Debate, 6—9—13, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined>, accessed 10-4-13. The question raises a real paradox. If government can keep secrets, then the public cannot hold it to account for its actions. But if government cannot keep secrets, then many programs — including highly desirable ones — are impossible. Many commentators seem to think that the answer is to keep secrecy to an absolute minimum, but this response is far too easy. One reason it is too easy is that it implies that secrecy can be exceptional. Government secrecy in fact is ubiquitous in a range of uncontroversial settings. To do its job and protect the public, the government must promise secrecy to a vast range of people — taxpayers, inventors, whistle-blowers, informers, hospital patients, foreign diplomats, entrepreneurs, contractors, data suppliers and many others. But that means that the basis of government action, which relies on information from these people, must be kept secret from the public. Economic policy is thought to be open, but we saw during the financial crisis that government officials needed to deceive the public about the health of the financial system to prevent self-fulfilling runs on banks. Then there are countless programs that are not secret but that are too complicated and numerous for the public to pay attention to — from E.P.A. regulation to quantitative easing. N.S.A. surveillance blends into this incessant, largely invisible background buzz of government activity; there is nothing exceptional about it. And this puts even more pressure on the first prong of the paradox. If much (most?) of government activity remains invisible to the public, how can democratic accountability work? The answer, I think, is that political accountability in modern, large-scale democracies rarely takes place through informed public monitoring of specific government programs and policies. A few discrete issues (abortion, same-sex marriage) aside, and not counting political scandals, the public largely votes on the basis of its pocketbook and its feeling of security. The political consequences of war, terrorist attacks and economic distress — all of which are publicly observable — keep officeholders in line, but they retain vast discretion to choose among means. Because some government officials are ill-motivated and others are incompetent, government abuse is inevitable, but it is the price we pay for a government large and powerful enough to regulate 300 million people. Think of the N.S.A. program as the security equivalent of the Affordable Care Act (which will unavoidably involve government monitoring of people’s medical care on the basis of bureaucratic procedures that no one understands): in both cases, we must prepare ourselves for the inevitable abuses that accompany a large, unwieldy, hard-to-monitor program, in order to obtain the (promised) benefits. Objections to the secrecy of the N.S.A. program are thus really objections to our political system itself, and, for all its flaws, there are no obviously superior alternatives.

Surveillance Desirable: Topshelf [cont'd]

5. These surveillance programs are better than the far more abusive alternatives

Bill Scher, Campaign for America's Future, "The Liberal Case for High-Tech NSA Surveillance," THE WEEK, 6—13—13, <http://theweek.com/article/index/245464/the-liberal-case-for-high-tech-nsa-surveillance>, accessed 10-13-13. Meanwhile, we have evidence that NSA surveillance is helping to prevent terrorist plots. Some challenge that evidence, and it's hard to definitively sift through the debate because much of the program remains secret. But at least it's actual evidence and not mere hypothesizing. Of course, America's record on civil liberties when faced with serious threats is poor. Grave abuses have repeatedly occurred in the name of panic, or just out of rank pursuit of political power. Whatever your ideology, it is understandable to approach this debate from a perspective of cynicism and strive to keep as much personal data out of the federal government's hands as possible. But what Greenwald and Co. fail to appreciate is how these modern technologies appear to be diminishing the temptation for abuses. We are not deporting or interning Muslims en masse. We are not infiltrating and disrupting Tea Party meetings (delicate sensitivities about those having to wait a bit for tax-exempt status aside) despite multiple incidents of far-right domestic terrorism. Instead, we are employing cutting-edge technology in an effort to pinpoint actual terrorists. The NSA's current method of surveillance is government action on behalf of the common good, which to date has not produced any substantive infringement on personal freedom. It is part of an overall counterterrorism approach that is profoundly superior to past administrations' records in regards to protecting our civil liberties. President Obama is not violating his liberal principles by defending the NSA. He is exercising them.

Surveillance Desirable: Public Supports / Accepts

1. The NSA is not to blame—the program exists because the public wants to be protected from terror groups

Paul R. Pillar, Brookings Institution, "Stop Bashing the NSA," NATIONAL INTEREST, 8—1—13, <http://www.brookings.edu/research/opinions/2013/08/01-stop-bashing-nsa-pillar>, accessed 10-2-13.

This phenomenon can arise with any government component, but intelligence agencies seem especially liable to be viewed in this misplaced way. Scott Shane of the New York Times observes that U.S. intelligence agencies "have entered a period of broad public scrutiny and skepticism," citing controversies over interrogation and drone strikes as well as the more recent attention to electronic surveillance. The fact that these agencies, by mission and charter, do not make policy means that any perceptions that they are the drivers of whatever policy is the subject of controversy are very likely incorrect. The secrecy that surrounds these agencies and contributes to ignorance about them is another factor, although occasionally journalists shed corrective light on the subject, as Walter Pincus of the Washington Post has done with regard to the specific NSA-implemented electronic collection programs that are at the center of the most recent controversies. Those programs do not exist because someone at NSA thought it would be nifty to expand the agency's operations by doing something like that. They exist because the American public—with its desires and demands expressed through the political branches of government—wanted vigorous intelligence efforts on behalf of counterterrorism and because the technology is such that large-scale electronic collection is one of the most promising ways of making such efforts. NSA is implementing the programs because it is the component that happens to have the mission and capability to do such things. The purpose, general parameters and limitations of the programs all have been set outside the agency. The specific operational designs are the work of NSA, but any design that was not intensive and extensive would not have delivered the expected vigor.

2. These surveillance programs are necessary to protect us against terrorist threats, and most of the public agrees

Michael Barone, American Enterprise Institute, "NSA Surveillance, if Ungentlemanly, Is not Illegal," WASHINGTON EXAMINER, 6—11—13, <http://aei.org/article/foreign-and-defense-policy/defense/intelligence/nsa-surveillance-if-ungentlemanly-is-not-illegal/>, accessed 10-4-13.

You might think, as Henry Stimson did in 1929, that it's ungentlemanly. But as secretary of war between 1940 and 1946, Stimson was grateful for the code-breaking programs that enabled the United States and Britain to decrypt secret Japanese and German messages. That code breaking, as historians have recounted, though not until long after the war, undoubtedly saved the lives of tens of thousands of Allied service members. "The Constitution and U.S. laws," as former Attorney General Michael Mukasey wrote in the Wall Street Journal, "are not a treaty with the universe; they protect U.S. citizens." It is an interesting development that Barack Obama has continued and, Snowden asserts, strengthened programs at least some of which he denounced as a U.S. senator and presidential candidate. As George W. Bush expected, Obama's views were evidently changed by the harrowing contents of the intelligence reports he receives each morning. There are people out there determined to harm us, and not just because they can't bear Bush's Texas drawl. The Pew Research/Washington Post poll conducted from June 7 to 9 found that by a 56 to 41 percent margin, Americans found it "acceptable" that the "NSA has been getting secret court orders to track calls of millions of Americans to investigate terrorism." That's similar to the margin in a 2006 Pew poll on the NSA "secretly listening in on phone calls and reading emails without court approval." Those numbers are in line with changes in opinion over the last two decades. With increased computer use, technology is seen as empowering individuals rather than Big Brother. And with an increased threat of terrorist attack, government surveillance is seen as protecting individuals. In these circumstances, most Americans seem willing to accept NSA surveillance programs that, if ungentlemanly, are not illegal.

Surveillance Desirable: Public Supports / Accepts [cont'd]

3. There is no public backlash—reactions have been largely muted

David Rieff, "Why Nobody Cares About the Surveillance State," FOREIGN POLICY, 8—22—13, www.foreignpolicy.com/articles/2013/08/22/why_nobody_cares_about_the_surveillance_state_nsa, accessed 10-3-13. Despite anger at Snowden and apocalyptic claims by government officials that he had gravely undermined their ability to protect Americans from terrorist attacks, it turned out that the "secret" he revealed appeared to be one of the most broadly shared secrets in the world. The White House knew, members of the Senate and House intelligence committees knew, and major U.S. allies like Britain and Germany not only knew but in some cases collaborated in the effort. Companies like Apple, Google, and Microsoft may not have known everything, but unquestionably they knew something. The only group that did not know about PRISM was the general public. And yet, apart from some voices from the antiwar left and the libertarian right (on foreign policy there is considerable overlap between the Tea Party and the Occupy movement), the reaction from this deceived public for the most part has been strangely muted. It is not just the somewhat contradictory nature of the polls taken this summer, which have shown the public almost evenly split on whether the seemingly unlimited scope of these surveillance programs was doing more harm than good. It is also that, unlike on issues such as immigration and abortion, much of the public outrage presupposed by news coverage of the scandal does not, in reality, seem to exist.

4. The public has largely accepted that they have no privacy online—explains lack of concern over the NSA programs

David Rieff, "Why Nobody Cares About the Surveillance State," FOREIGN POLICY, 8—22—13, www.foreignpolicy.com/articles/2013/08/22/why_nobody_cares_about_the_surveillance_state_nsa, accessed 10-3-13. The truth is that whether it is in the service of emancipation or repression, most people who have access to the new Internet and other communications technologies can no longer really imagine living without them. They feel -- and in many important ways they are -- not just pleasurable but empowering. At the same time, except for some hackers and programmers, this pleasure and empowerment comes only at the discretion of governments and those corporations that control the biggest computers in a network. The pioneer of virtual-reality technology turned critic of digital utopianism, Jaron Lanier, put it well when he said that "every time you post a tweet attacking the 1 percent, you enrich some member of the 1 percent." For most people, privacy, too, has become the "shining artifact of the past" that Leonard Cohen once sang about. Indeed, anyone with a mobile phone understands that everything from their bank records to the products they buy online to the telephone numbers they dial and the addresses to which they send emails are recorded somewhere -- whether by a private business, their own employers, or, of course, the government. Viewed from this perspective, is it the general public's comparative lack of indignation over the NSA surveillance scandal that is surprising, or is the real shocker that journalists, activists, and politicians feel so outraged? Yes, the U.S. government is indeed the Biggest Brother of them all, but most people go about their daily business being spied on and having their data mined by any number of small- and medium-sized brothers. Of course, someone who is outraged by the attempts to jail the leakers and prosecute and intimidate their journalist and activist colleagues would insist, and rightly so, that these sorts of things should not be permitted in a democracy. But the gap between the outrage of the chattering classes and the public's apathy -- or, more likely, resignation -- illuminates the essential difference between the elite's understanding of the world and everyone else's. To put it starkly, members of an elite tend to believe they can change things; most everyone else knows that, except in a few rare instances, they cannot. In an essential sense, the real question for members of the elite is not, why isn't the public outraged, but why are we?

Surveillance Desirable: Public Supports / Accepts [cont'd]

5. The surveillance state is inevitable, and the public has accepted this fact

David Rieff, "Why Nobody Cares About the Surveillance State," FOREIGN POLICY, 8—22—13, www.foreignpolicy.com/articles/2013/08/22/why_nobody_cares_about_the_surveillance_state_nsa, accessed 10-3-13. It is important to be clear. Does the public take the revelations of the data-mining scandal as an affront to their liberty? Presumably many, perhaps even most, do. But life is so full of affronts about which one would be an utter fool to imagine that one can do anything. The automated recordings through which one so often has to pay one's bills, arrange an appointment, or try to get information (even whom to speak with to get that information) are an affront. The endless passwords, PINs, and the like are an affront (and are also, by definition, recorded on corporate databases). The ubiquitous CCTV cameras in city centers, a great many of which were installed well before the Sept. 11 attacks as crime-prevention and traffic-control measures, are an affront. And of course, all the petty and not so petty inconveniences and impositions of the post-9/11 world -- from the preposterous demand that one show ID when entering not just a government building but almost any office building in America, to the shameless slovenliness and rudeness of Transportation Security Administration employees at every U.S. airport -- are flagrant affronts. Even if the long war against the jihadis were to end tomorrow with total victory for the United States, can anyone seriously suggest that any of these measures would be lessened, let alone canceled? The great myth of the past 25 years may be empowerment through technology. But the great truth of the past 25 years has been the rise of the surveillance state, which grows stronger every day -- both because of technology itself and because of the control that states and huge corporations have over the technology that people depend upon and love. On one level, everyone knows this, but whether it's because they believe themselves to be immune or because they simply never imagined that the surveillance state had become so all-encompassing, the elites seem to have been particularly surprised and therefore indignant over the scope of the NSA's spying, the ardor with which governments have defended these practices, and their foaming rage at having to defend them in public at all. "This is the way the world ends," T. S. Eliot famously wrote in his great poem *The Hollow Men*, "not with a bang but a whimper." Welcome to the post-democratic world. Oh, and by the way, you've been living in it for quite some time now.

Surveillance Desirable: Terror—Topshelf

1. NSA intelligence programs are one of the only viable tools we have to stop terror attacks

Marc A. Thiessen, American Enterprise Institute, "Big Brother Isn't Watching You," WASHINGTON POST, 6—10—13, <http://aei.org/article/foreign-and-defense-policy/terrorism/big-brother-isnt-watching-you/>, accessed 10-3-13.

If the critics don't think the NSA should be collecting this information, perhaps they would like to explain just how they would have us stop new terrorist attacks. Terrorists don't have armies or navies we can track with satellites. There are only three ways we can get information to prevent terrorist attacks: The first is interrogation — getting the terrorists to tell us their plans. But thanks to Barack Obama, we don't do that anymore. The second is penetration, either by infiltrating agents into al-Qaeda or by recruiting operatives from within the enemy's ranks. This is incredibly hard — and it got much harder, thanks to the leak exposing a double agent, recruited in London by British intelligence, who had penetrated al-Qaeda in the Arabian Peninsula and helped us break up a new underwear bomb plot in Yemen — forcing the extraction of the agent. That leaves signals intelligence — monitoring the enemy's phone calls and Internet communications — as our principal source of intelligence to stop terrorist plots. Now the same critics who demanded Obama end CIA interrogations are outraged that he is using signals intelligence to track the terrorists. Well, without interrogations or signals intelligence, how exactly is he supposed to protect the country?

2. The NSA's programs are important in checking terror plots—expert survey proves

Sara Sorcher, "Insiders: NSA's Communications Surveillance Good Way to Target Terrorists," NATIONAL JOURNAL, 6—24—13, www.nationaljournal.com/insiders-polls/nationalsecurity/insiders-nsa-s-communications-surveillance-good-way-to-target-terrorists-20130624, accessed 10-2-13.

The National Security Agency's surveillance programs are effective tools for seeking out terrorists, according to 85.5 percent of National Journal's National Security Insiders. "In the digital age, when every individual's digital trail increases year by year, there is no faster way to draw a picture of a network, or a conspiracy, than by piecing together different data streams," one Insider said. "This capability, in years to come, won't be a nice-to-have; it'll be critical." Another Insider said that the NSA must have the tools necessary to root out terrorists or another 9/11 becomes not just possible, but certain. "If we eliminate the online- and phone-surveillance programs and a dirty bomb explodes in an American city, we have only ourselves to blame," the Insider said. "The days of gentlemen not reading other gentlemen's mail are over." Some Insiders note that individual identities and habits are already tracked intensely in the commercial sphere. "I have been fingerprinted at Disneyland and Universal Studios," one said. "When you board a plane in the U.K., your picture is taken before you get on. When you cross a border into the U.S., video is taken of your license plate. Cruise ships require photo IDs be made. Amazon and Google have consumer avatars created for customers and users. Financial institutions routinely collect and track data on customers. When we drive over sensors on a road they collect metadata to establish patterns to improve flow and safety. Whatever NSA may be doing pales in scale to what is happening in plain view."

3. Surveillance is vital to checking the threat posed by Al Qaeda

Marc Thiessen, "Why We Need NSA Surveillance: RAND Study Finds Al Qaeda Expanding," AEI IDEAS, American Enterprise Institute, 7—23—13, www.aei-ideas.org/2013/07/why-we-need-nsa-surveillance-rand-study-finds-al-qaeda-expanding/, accessed 10-2-13.

Of course, this was precisely the intelligence community's view back in 2009 of al Qaeda's new affiliate in Yemen — that it was focused on regional attacks and had no interest in America. That is, until it sent a terrorist with an underwear bomb to blow up a Northwest Airlines flight over Detroit on Christmas Day. Disaster was averted only because the bomb malfunctioned. Later, in the aftermath of that attack, the Obama administration admitted it did not know that al Qaeda in the Arabian Peninsula had developed the capability and intent to strike the American homeland. Prudence dictates that we not make the same mistake again, and assume that al Qaeda's growing network of affiliates and allies does not possess the intent or capability of striking us at home. Of course, the best way to ensure we are not taken by surprise again is to actively monitor the communication of these terrorist networks. The fact is, al Qaeda is not decimated, it is growing. And if we want to find out what they are planning, we need to maintain a robust NSA terrorist surveillance program.

Surveillance Desirable: Terror—Allies

- The NSA programs make it easier for our allies to catch terrorists abroad

Sebastian Rotella, Pulitzer Prize winning journalist, “How the NSA’s High-Tech Surveillance Helped Europeans Catch Terrorists,” PROPUBLICA, 6—19—13, www.propublica.org/article/how-the-nas-high-tech-surveillance-helped-europeans-catch-terrorists, accessed 10-4-13.

As debate rages in the United States about the National Security Agency’s sweeping data-mining programs, I’ve been on a reporting trip overseas, where I’ve been talking to sources about the controversy and how differing U.S. and European approaches to counterterrorism can complement each other. On Tuesday, NSA Director Gen. Keith Alexander, told a congressional committee that his agency’s surveillance programs helped stop more than 50 terror plots in the U.S. and abroad. Five years ago, I was based in Europe covering terrorism, running from one attack or aborted plot to another. As the Brussels investigation shows, these cases frequently combined the high-tech reach of the U.S. counterterror apparatus with the street skills of foreign agencies. In November 2008, Pakistani and U.S. agents swooped into Kandahar and nabbed Bryant Neal Vinas, the convert from Long Island and al-Qaida militant. He cooperated with the FBI, admitting that he discussed an attack on the Long Island Rail Road with top al-Qaida figures. Days later, a drone strike killed Rashid Rauf, a Pakistani-British operative who helped plan the London transport bombings and the “liquid bomb” plot to blow up planes in 2006. Three Belgian and French militants returned home, where police arrested them after intercepts picked up menacing chatter. Vinas pleaded guilty. Aroud went to prison, and investigators believe her second husband Garsallaoui died in the land of jihad. Other cases benefited from close cooperation. In Germany in 2007, U.S. monitoring detected a suspect checking the draft file of an email box at an Internet cafe in Stuttgart. Armed with that lead, German security services deployed surveillance at numerous Internet cafes in the city. The investigation resulted in the dismantling of a Pakistan-trained group plotting to attack U.S. military targets in Germany. As several European sources told me, if an extremist in Marseilles was talking about nefarious activities with an extremist in Geneva over the Internet, chances were good that U.S. intelligence agencies would find out and inform the French and Swiss. Not because of sources on the ground, but because U.S. agencies could detect the communications through computer servers in the United States. The reaction here to the U.S. debate has been bemused. European terrorist hunters seem surprised that the revelation of the NSA data-monitoring programs is big news. The technological capacities of U.S. agencies have been an integral component of dramatically improved teamwork against terrorism during the past decade. “In the fight against terrorism, intelligence-sharing is essential,” said Jean-Louis Bruguière, who served for more than two decades as a top French antiterror magistrate before retiring in 2007. (He declined to discuss the NSA’s role in investigations.) “Cooperation with American services has always been trusting and excellent.”

Surveillance Desirable: Terror—Bush Era Programs

1. Bush-era NSA programs foiled terror attacks

John Yoo, Professor, Law, University of California, Berkeley, “The Terrorist Surveillance Program and the Constitution,” *GEORGE MASON LAW REVIEW* v. 14, 2007, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=975333, accessed 10-2-13.

No one—even the critics—seems to doubt that the information gained from the NSA program has led to the successful prevention of al Qaeda plots against the United States. According to General Michael Hayden, President Bush’s nominee to head the CIA and leader of the NSA during much of the program’s existence, “[t]his program has been successful in detecting and preventing attacks inside the United States.” When pressed by reporters whether it had succeeded where no other method would have, he said, “I can say unequivocally, all right, that we have got information through this program that would not otherwise have been available.” Attorney General Alberto Gonzales informed the press that the NSA program was perhaps the most classified program in the U.S. government, and that it had helped obtain information that had prevented attacks within the United States. The main criticism has not been that the program is ineffective, but that it violates the Constitution and cannot be undertaken, no matter how successful or necessary to protect the public.

2. We need to move beyond traditional conceptions of surveillance to foil organizations like Al Qaeda

John Yoo, Professor, Law, University of California, Berkeley, “The Terrorist Surveillance Program and the Constitution,” *GEORGE MASON LAW REVIEW* v. 14, 2007, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=975333, accessed 10-2-13.

Al Qaeda, our current enemy, poses a very different challenge. We do not have a list of diplomats to work from or an embassy to watch, as was the dominant paradigm in the Cold War. An intelligence search conducted today, as Judge Richard Posner has described it, “is a search for a needle in a haystack.” Rather than focus on foreign agents who are already known, counter-terrorism agencies must search for clues among millions of potentially innocent connections, communications, and links. “The intelligence services,” Posner writes, “must cast a wide net with a fine mesh to catch the clues that may enable the next attack to be prevented.” Our best information about al Qaeda will be scattered and tough to gather, and our agents must be able to follow many leads quickly and move fast on hunches and educated guesses. Members of the al Qaeda network can be detected, with good intelligence work or luck, by examining phone and e-mail communications, as well as evidence of joint travel, shared assets, common histories or families, meetings, and so on. As the time for an attack nears, “chatter” on this network will increase as al Qaeda operatives communicate to coordinate plans, move and position assets, and conduct target reconnaissance. When our intelligence agents successfully locate or capture an al Qaeda member, they must be able to move quickly to connect new information to other operatives before news of the capture causes these operatives to disappear. It is more important to chase them down quickly inside the United States than outside. Incredibly, critics want to place bureaucratic impediments precisely at this juncture, where the danger to America is greatest.

Surveillance Desirable: Terror—Empirically True

1. Current surveillance programs have foiled dozens of terrorist attacks

Steven Bucci, “Phone Records and the NSA: Legal and Keeping America Safe,” THE FOUNDRY, Heritage Foundation, 6—20—13, <http://blog.heritage.org/2013/06/20/phone-records-and-the-nsa-legal-and-keeping-america-safe/>, accessed 10-3-13. Moreover, NSA Director General Keith Alexander testified to Congress that these surveillance programs have helped foil dozens of terrorist attacks. These include, he stated, an attempted suicide plot against the New York City subway system by Najibullah Zazi, who pleaded guilty. Since 9/11, the U.S. has thwarted over 50 terrorist plots against America’s homeland. In addition to continued reliance on counterterrorism devices such as the Patriot Act and the NSA surveillance programs, Congress must take action to plug the remaining gaps in our counterterrorism system. For instance, there should be increased visa coordination to prevent known terrorists from boarding airplanes and travelling to the U.S. Additionally, Congress should foster greater cooperation among local, state, and federal agencies to streamline their information-sharing capabilities. The current debate raging over Snowden’s leaking of the secret NSA surveillance program is no doubt a healthy exercise for a thriving democracy. The scope of the metadata collection and how the government uses it should come under close scrutiny. However, Congress and the American people should understand that these programs—which are under judicial, executive, and legislative oversight—are vital tools for law enforcement and intelligence officials in countering the ongoing threat of terrorism.

2. The NSA program stops terror plots—recent examples prove

Michael Chertoff, former Director, Homeland Security, “NSA Surveillance Vital to Our Safety,” USA TODAY, 9—11—13, www.usatoday.com/story/opinion/2013/09/11/nsa-privacy-chertoff-911-column/2793063/, accessed 10-4-13. For example, according to public reports, recently disclosed NSA programs led U.S. officials to connect an email about a recipe for explosives with a known terrorist located in Pakistan. When seeking to find out with whom the terrorist was in contact, intelligence officials discovered Najibullah Zazi, an Afghan-American residing at the time in Colorado who was planning to blow up the New York subway system. If this plot had not been discovered, many believe it would have been the biggest terrorist attack on U.S. soil since 9/11. In January 2009, the NSA used authorized capabilities to monitor the communications of an extremist overseas with ties to al-Qaeda and discovered a connection with an individual in Kansas City. This information was provided to the FBI who through their investigation discovered a plot to attack the New York Stock Exchange. In both cases, the NSA was able to connect known al-Qaeda associates with individuals plotting an attack here in the United States. Twelve years after 9/11, we have made tremendous progress in strengthening security to prevent threats from reaching our shores as well as detecting those who have already infiltrated our nation. We also face a more dangerous enemy. The al-Qaeda we once knew as a central, integrated terrorist organization has morphed into a widely dispersed new generation of fighters seeking to launch attacks from a much wider region of operations. While their ability to repeat large-scale, iconic attacks largely has been diminished, these operatives are willing to take more risks today and attempt smaller scale operations that still pose a serious danger to U.S. interests around the world. To be sure, we should periodically revisit our intelligence authorities to assure that they are not unduly and unnecessarily intrusive. In fact, several times since 9/11, Congress and the Foreign Intelligence Surveillance Court have modified the rules of intelligence collection to balance security and privacy interests. There are ways to adjust the current regime for storing meta data, for example, so as to afford more transparency and assurance against abuse. But we should not call into question the fundamental contribution that signals intelligence makes to our safety. Without a global ability to swiftly identify known and unknown threats heading our way in the future, we will have more unhappy anniversaries like September 11.

Surveillance Desirable: Terror—Empirically True [cont'd]

3. Four examples prove that the NSA programs are important in checking terrorist plots

Marshall Curtis Erwin, and Edward C. Liu, Congressional Research Service, “NSA Surveillance Leaks: Background and Issues for Congress,” CRS REPROT FOR CONGRESS, 7—2—13, p. 10-11.

According to intelligence officials, the two programs have “helped prevent over 50 potential terrorist events”—which appear to encompass both active terror plots targeting the United States homeland and terrorism facilitation activity not tied directly to terrorist attacks at home or abroad. Of these, over 90% somehow involved collection pursuant to Section 702. Of the 50, at least 10 cases included homeland-based threats, and a majority of those cases somehow utilized the phone records held by NSA. The Administration has provided four examples: • Najibullah Zazi: NSA, using 702 authorities, intercepted an email between an extremist in Pakistan and an individual in the United States. NSA provided this email to the FBI, which identified and began to surveil Colorado-based Najibulla Zazi. NSA then received Zazi’s phone number from the FBI, checked it against phone records procured using 215 authorities, and identified one of Zazi’s accomplices, an individual named Adis Medunjanin. Zazi and Medunjanin were both subsequently arrested and convicted of planning to bomb the New York City subway. Additional information on this case is offered in the next section. • Khalid Ouazzani: NSA, using 702 authorities, intercepted communication between an extremist in Yemen and an individual in the United States named Khalid Ouazzani. Ouazzani was later convicted of providing material support to al-Qaeda and admitted to swearing allegiance to the group. The FBI has claimed that Ouazzani was involved in the early stages of a plot to bomb the New York Stock Exchange. • David Headley: According to intelligence officials, the FBI received information indicating that Headley, a U.S. citizen living in Chicago, was involved in the 2008 attack in Mumbai that took the lives of 160 people. NSA, using 702 authorities, also became aware of Headley’s involvement in a plot to bomb a Danish newspaper. It is unclear from public statements how Headley first came to the FBI’s attention. He pled guilty to terrorism charges and admitted to involvement in both the Mumbai attack and Danish newspaper plot. • Basaaly Saeed Moalin: NSA, using phone records pursuant to 215 authorities, provided the FBI with a phone number for an individual in San Diego who had indirect contacts with extremists overseas. The FBI identified the individual as Basaaly Saeed Moalin and determined that he was involved in financing extremist activity in Somalia. Moalin was convicted in 2013 of providing material support to al-Shabaab, the Somalia-based al-Qaeda affiliate.

4. The programs have already stopped 50 terrorist attacks

Karuna Chandwani, “PRISM Helped Dodge Over 50 Terror Attacks,” INTERNATIONAL BUSINESS TIMES, 6—19—13, www.ibtimes.co.in/articles/480569/20130619/nsa-chief-hearing-prism-national-security-agency.htm, accessed 10-12-13. The chief of United States National Security Agency (NSA) has justified the activities of its PRISM surveillance program saying it has helped fend off many terrorist attacks within the country and abroad since the September 9/11 attack. At a rare public hearing in Washington, NSA Director Keith Alexander said that more than 50 terrorist attacks in over 20 countries were prevented by data collected through phone records (section 215 of the FISA Amendments Act) or 'business records' including emails (section 702). The disrupted attacks include 'little over 10' plots with a 'domestic nexus'. FBI Deputy Director Sean Joyce described four declassified instances where NSA's surveillance prevented terror plots by arresting the accused including the capture of David Headley, the accused in the 26/11 Mumbai attack.

5. NSA surveillance is responsible for stopping dozens of terror plots

Steven Bucci, “NSA Spying Stops Terrorism but Should Also Respect Liberties,” THE FOUNDRY, Heritage Foundation, 6—18—13, <http://blog.heritage.org/2013/06/18/nsa-spying-stops-terrorism-but-should-also-respect-liberties/>, accessed 10-3-13. General Keith Alexander, the director of the National Security Agency (NSA), testified in an open hearing before the House Permanent Select Committee for Intelligence on how intelligence collection supports the national effort to fight transnational terrorism. For the first time, he revealed that more than 50 incidents of potential terrorism were stopped by the set of programs under scrutiny. He emphasized that he was working to declassify these incidents so they could be shared with the American people. These revelations come as no surprise to us. Heritage research has noted 54 foiled terrorist plots since 9/11. Given that we know of only three that were not stopped by intelligence (the shoe bomber, the underwear bomber, and the Times Square bomber), this means that these NSA programs might well have played a significant role in thwarting dozens of uncovered plots. Heritage has long held that tools such as the PATRIOT Act and legitimate surveillance programs can be important tools for battling transnational terrorism.

Surveillance Desirable: Terror—Empirically True [cont'd]**6. The programs have foiled 50 terror plots**

Steven Nelson, "NSA Director: Surveillance Stopped 50 Terror Plots," U.S. NEWS & WORLD REPORT, 6—18—13, www.usnews.com/news/newsgram/articles/2013/06/18/nsa-director-surveillance-stopped-50-terror-plots, accessed 10-2-13. National Security Agency Director Keith Alexander testified Tuesday before the House Intelligence Committee that phone and Internet surveillance programs made public by former defense contractor Edward Snowden prevented approximately 50 terrorist plots since 2001, 10 of which targeted the U.S., and said new policies are being crafted to prevent another large-scale leak. Alexander disclosed that approximately 1,000 people are currently employed as NSA systems administrators – the position Snowden held – and that the agency is "working to come up with a two-person rule" to prevent people "from taking information out of our system." Snowden was a contractor assigned to the NSA by Booz Allen Hamilton before he downloaded and released information on the top-secret programs. The intelligence agency leader didn't go into detail about what precisely the new "two person" rule would entail. "When one of those persons misuses their authority, that is a huge problem," Alexander said. The government officials present at Tuesday's hearing publicly disclosed two cases they said were cracked with the broad communications surveillance: One in 2010, in which investigators nabbed Khalid Ouazzani for allegedly plotting with Yemeni co-conspirators to blow up the New York Stock Exchange and another in which a man was arrested for providing "financial support" to an extremist group in Somalia.

Surveillance Desirable: Terror—Key to Prevention

1. The program is necessary to protect us from terror attacks

WALL STREET JOURNAL, "Thank You for Data-Mining," 6—7—13,

<http://online.wsj.com/news/articles/SB10001424127887324299104578529373994191586>, accessed 10-12-13.

Well, another day, another Washington furor. This one is over a National Security Agency phone data monitoring program, but unlike the other White House scandals there seems to be little here that is scandalous. The existence of the program was exposed years ago and such surveillance is a core part of the war on terror, if we can still use that term. Someone leaked a classified three-page order from the special court established by the Foreign Intelligence Surveillance Act, or FISA, to Glenn Greenwald of the Guardian newspaper, who is a committed anti-antiterror partisan. The warrant instructs a business unit of Verizon to turn over its call logs for any communications "between the United States and abroad" or "wholly within the United States, including local telephone calls." Such "telephony metadata" are records such as which number called which number and when, where the call was placed, its duration, etc. This does not include the content of the communications. Presumably such orders went to other parts of Verizon and other telecom carriers as well. USA Today reported the program in detail in 2006, while James Bamford wrote a long Wired magazine cover story about it last year.

2. NSA work is vital to stopping terror attacks

Max Boot, senior fellow, Council on Foreign Relations, "Stay Calm and Let the NSA Carry On," LOS ANGELES TIMES, 6—9—13, <http://articles.latimes.com/2013/jun/09/opinion/la-oe-boot-nsa-surveillance-20130609>, accessed 10-4-13.

After 9/11, there was a widespread expectation of many more terrorist attacks on the United States. So far that hasn't happened. We haven't escaped entirely unscathed (see Boston Marathon, bombing of), but on the whole we have been a lot safer than most security experts, including me, expected. In light of the current controversy over the National Security Agency's monitoring of telephone calls and emails, it is worthwhile to ask: Why is that? It is certainly not due to any change of heart among our enemies. Radical Islamists still want to kill American infidels. But the vast majority of the time, they fail. The Heritage Foundation estimated last year that 50 terrorist attacks on the American homeland had been foiled since 2001. Some, admittedly, failed through sheer incompetence on the part of the would-be terrorists. For instance, Faisal Shahzad, a Pakistani American jihadist, planted a car bomb in Times Square in 2010 that started smoking before exploding, thereby alerting two New Yorkers who in turn called police, who were able to defuse it. But it would be naive to adduce all of our security success to pure serendipity. Surely more attacks would have succeeded absent the ramped-up counter-terrorism efforts undertaken by the U.S. intelligence community, the military and law enforcement. And a large element of the intelligence community's success lies in its use of special intelligence — that is, communications intercepts. The CIA is notoriously deficient in human intelligence — infiltrating spies into terrorist organizations is hard to do, especially when we have so few spooks who speak Urdu, Arabic, Persian and other relevant languages. But the NSA is the best in the world at intercepting communications. That is the most important technical advantage we have in the battle against fanatical foes who will not hesitate to sacrifice their lives to take ours.

3. Foreign surveillance is entirely justified

Tim Worstall, "NSA's PRISM Sounds Like a Darn Good Idea to Me," FORBES, 6—7—13,

www.forbes.com/sites/timworstall/2013/06/07/nsas-prism-sounds-like-a-darn-good-idea-to-me-this-is-what-governments-are-for/, accessed 10-2-13.

That the NSA is looking at as much information and data it can get on what those nefarious foreigners are up to outside the US doesn't seem objectionable to me in the slightest. Indeed, I rather think that that's the purpose of government, to protect us, and it's the reason we hire the spies in the first place. They're doing exactly what they should be: looking for those who would do us, the citizenry, harm and then attempting to prevent them doing so. Sure, the foreigners aren't going to be very happy about it all: but their own governments (or perhaps I should say "ours") are doing as much of it to US citizens as they can. The dividing line, the where it moves from being entirely reasonable and sensible to being an outrage that must be prevented, is when governments do this sort of thing to their own citizens.

Surveillance Desirable: Terror—Key to Prevention [cont'd]

4. SIGINT is a vital tool in stopping terrorist attacks

Max Boot, fellow, Council on Foreign Relations, “‘Top Secret’ Should Mean Just That,” COMMENTARY, 6—6—13, www.commentarymagazine.com/2013/06/06/top-secret-should-mean-just-that/#more-826751, accessed 10-12-13.

I have no idea who this intelligence officer is, but he (or she) has committed a serious crime by the unauthorized disclosure of such sensitive information. He needs to be ferreted out and prosecuted. Perhaps if he had actual knowledge of the PRISM program being misused such a breach of confidentiality might be morally, if not legally, justifiable—although even then his first step should be to contact his superiors or others in the government, not to talk to the Washington Post. But there is no suggestion of such misuse here. Instead this appears to be another legal and authorized program that has been implemented by our elected leaders to protect us against terrorists. Government officials stress that only “non-U.S. persons” who are abroad are subject to PRISM monitoring and that the entire program was authorized by the 2007 Protect America Act. President Obama deserves to be commended for continuing these programs, building on work done in the Bush administration, rather than being attacked as the second coming of Big Brother. The Post and Guardian, for their part, are being irresponsible by printing these disclosures that are more highly classified than the cables that Bradley Manning released—a crime for which he is now being tried. Instead of expressing outrage at these actions to fight terrorism, as so many on both the left and right are now doing, it would be nice if someone got a little outraged at this breach of the secrecy needed for effective intelligence-gathering. It seems like only yesterday that the chattering classes were castigating the FBI, CIA and other agencies for not doing a better job of monitoring the Tsarnaev brothers before they carried out the Boston bombing. Similar outrage is being directed at the British security services in the wake of their failure to prevent the murder of a British soldier by two Anglo-Nigerian jihadists. Obviously “sigint” collection tools such as PRISM are not a foolproof defense against such attacks especially when undertaken by loners unaffiliated with a known terrorist organization. But they are an important, indeed vital, tool to prevent major attacks on a 9/11 scale, which require far more planning and organization. Exposing these collection tools makes it harder for them to be effective; shutting them down would amount to unilateral disarmament in the face of a continuing terrorist assault.

5. The programs exist because they work in stopping terrorist attacks

Joshua Foust, former analyst, Defense Intelligence Agency, “Secrecy and Freedom,” NEW YORK TIMES, Room for Debate, 6—9—13, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined>, accessed 10-4-13.

While debating the morality and ultimate legality of last week’s N.S.A. revelations is important, it is also important to realize why programs like collecting telephone metadata and Prism exist to begin with. In short: people think it works. News stories from 2002 show that the public was demanding the intelligence community “do more” to analyze information and thwart any future terrorist attacks. As a result, many of the barriers between domestic law enforcement and intelligence agencies, built after the 1975 Church Committee hearings, have been removed to make investigations easier. Has removing the “wall” actually helped to prevent terrorist attacks? Anonymous government sources have advanced the claim that Prism – a workflow management tool misreported as a means for collecting information – was instrumental in stopping Najibullah Zazi, who had planned on bombing the New York subway system. Those claims are disputed, at least in part, by public records of the Zazi case. It’s unclear whether there are other success stories that matter in this debate. The high level of secrecy around these programs – all have been marked “NOFORN,” meaning no foreign national should ever read about them – makes discussing their effectiveness extraordinarily difficult. The government, too, faces a Catch-22 in defending itself: discussing the success of these programs would, by design, require removing secrecy about them. If they only work because they’re secret, then that’s a tough choice to make. At a political level, too, the effectiveness argument is vitally important. Director of National Intelligence James Clapper has called the leaks “literally gut-wrenching,” not because he is an evil man who loves violating privacy laws but because he seems to genuinely believe those exposed programs work. The Senate Intelligence Committee chairwoman, Diane Feinstein, too, has claimed that the N.S.A. effectively disrupts terror attacks.

Surveillance Desirable: Terror—Key to Prevention [cont'd]

6. Intel is the best tool we have available to stop attacks against the U.S.

John Yoo, Professor, Law, University of California, Berkeley, "The Terrorist Surveillance Program and the Constitution," *GEORGE MASON LAW REVIEW* v. 14, 2007, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=975333, accessed 10-2-13.

Gathering intelligence has long been understood as a legitimate aspect of conducting war; indeed, it is critical to the successful use of force. Our military cannot attack or defend to good effect unless it knows where to aim. America has a long history of conducting intelligence operations to obtain information on the enemy. General Washington used spies extensively during the Revolutionary War, and as President he established a secret fund for spying that existed until the creation of the CIA. President Lincoln personally hired spies during the Civil War, a practice which the Supreme Court upheld. In both World Wars I and II, Presidents ordered the interception of electronic communications leaving the United States. Some of America's greatest wartime intelligence successes have involved SIGINT, most notably the breaking of Japanese diplomatic and naval codes during World War II, which allowed the U.S. Navy to anticipate the attack on Midway Island. SIGINT is even more important in this war than in those of the last century. Al Qaeda continues to launch a variety of efforts to attack the United States, including acquiring and deploying weapons of mass destruction. The primary way to stop those attacks is to locate and stop al Qaeda operatives who have infiltrated the United States. One way to find them is to intercept their electronic communications entering or leaving the country.

7. NSA-style programs are the only way to track potential terrorists

Stewart Baker, former Assistant Secretary for Policy, Department of Homeland Security, "Why the NSA Needs Your Phone Calls," *FOREIGN POLICY*, 6—6—13, www.foreignpolicy.com/articles/2013/06/06/why_the_nsa_needs_your_phone_calls, accessed 10-12-13.

But why, you ask, would the government collect all these records, even subject to minimization, especially when Wyden was kicking up such a fuss about it? And, really, what's the justification for turning the data over to the government, no matter how strong the post-collection rules are? To understand why that might seem necessary, consider this entirely hypothetical example. Imagine that the United States is intercepting al Qaeda communications in Yemen. Its leader there calls his weapons expert and says, "Our agent in the U.S. needs technical assistance constructing a weapon for an imminent operation. I've told him to use a throwaway cell phone to call you tomorrow at 11 a.m. on your throwaway phone. When you answer, he'll give you nothing other than the number of a second phone. You will buy another phone in the bazaar and call him back on the second number at 2 p.m." Now, this is pretty good improvised tradecraft, and it would leave the government with no idea where or who the U.S.-based operative was or what phone numbers to monitor. It doesn't have probable cause to investigate any particular American. But it surely does have probable cause to investigate any American who makes a call to Yemen at 11 a.m., Sanaa time, hangs up after a few seconds, and then gets a call from a different Yemeni number three hours later. Finding that person, however, wouldn't be easy, because the government could only identify the suspect by his calling patterns, not by name. So how would the NSA go about finding the one person in the United States whose calling pattern matched the terrorists' plan? Well, it could ask every carrier to develop the capability to store all calls and search them for patterns like this one. But that would be very expensive, and its effectiveness would really only be as good as the weakest, least cooperative carrier. And even then it wouldn't work without massive, real-time information sharing -- any reasonably intelligent U.S.-based terrorist would just buy his first throwaway phone from one carrier and his second phone from a different carrier. The only way to make the system work, and the only way to identify and monitor the one American who was plotting with al Qaeda's operatives in Yemen, would be to pool all the carriers' data on U.S. calls to and from Yemen and to search it all together -- and for the costs to be borne by all of us, not by the carriers. In short, the government would have to do it.

Surveillance Desirable: Terror—Metadata-Specific

1. Metadata makes it easier to find anomalies that will lead us to terrorist groups

James Jay Carafano, Vice President for Defense and Foreign Policy studies, Heritage Foundation, “Big Data, Big Brother: It’s a Big Deal,” NATIONAL REVIEW ONLINE, The Corner, 6—7—13,

<http://www.heritage.org/research/commentary/2013/6/big-data-big-brother-its-a-big-deal>, accessed 10-4-13.

The world of big data, collecting massive amounts of information and the figuring out ways to sort through the stuff and use it, is only going to get bigger. It can also be pretty much guaranteed that the U.S. intelligence community will be a big consumer of big data. Last year, Steve Cambone, the former under secretary of defense for intelligence, led a team of top former intelligence officials in a sweeping review of the future of the community. The No. 1 challenge they outlined was dealing with big data. The report primarily addresses open-source data, information that is publicly available to anyone, but big data is also going to include personally identifying information and information constitutionally protected under the Bill of Rights.

Cambone also made the case that big data is not an unreasonable intrusion or an inefficient way to address small problems. Sometimes the easiest way to find a needle is put more hay in the stack -- in other words, the greater the amount of data we look at, the more the anomalies stand out.

2. Metadata collection is legal and helps protect us from terror threats

Steven Bucci, “Phone Records and the NSA: Legal and Keeping America Safe,” THE FOUNDRY, Heritage Foundation, 6—20—13, <http://blog.heritage.org/2013/06/20/phone-records-and-the-nsa-legal-and-keeping-america-safe/>, accessed 10-3-13.

In the U.S., counterterrorism operations rely on tools such as the NSA surveillance program and are overseen by Congress, the executive branch, and the courts to prevent gross misconduct and overreach. Before Congress and the American public decide to throw the baby out with the bathwater, they must understand that these programs keep us safe and allow the U.S. to adapt to the ever-changing, and very real, terrorist threat. Over the past week, Snowden has inundated the world with details about the NSA collection of telephone records from companies such as Verizon. However, according to a FISA court order, Verizon was only ordered to hand over “metadata” of the calls it processed. Metadata refers to basic information, including telephone number, location, and duration of the call, and the court order does not authorize the government to access the content of such conversations. There is a growing body of legal precedent for the NSA program. In 1976 the Supreme Court upheld “the third party doctrine,” which states that anyone who voluntarily provides information to a third party, such as a telephone service provider, cannot object if it is later turned over to the government. What’s more, in 1979, the Supreme Court held in *Smith v. Maryland* that the government did not need a warrant to obtain phone record information as it did for the content of such communications. The information was not constitutionally protected because there was no true expectation of privacy. As a result, metadata collection is not protected under the 4th Amendment and is perfectly legal. U.S. law enforcement and Intelligence agencies depend on tools and methods, such as the leaked NSA program, to combat homegrown radicalization and to fight the ongoing threat from terrorist cells such as the Al-Qaeda in the Arabian Peninsula in Yemen.

3. Using metadata is more effective and cost-efficient than analyzing individual calls

Edward W. Felten, Professor, Computer Science and Public Affairs, Princeton University, Testimony before the Senate Intelligence Committee, 10—2—13, <http://www.judiciary.senate.gov/pdf/10-2-13FeltenTestimony.pdf>, accessed 10-8-13.

The contents of calls are far more difficult to analyze in an automated fashion due to their unstructured nature. The NSA would first have to transcribe the calls and then determine which parts of the conversation are interesting and relevant. Assuming that a call is transcribed correctly, the NSA must still try to determine the meaning of the conversation: When a surveillance target is recorded saying “the package will be delivered next week,” are they talking about an order they placed from an online retailer, a shipment of drugs being sent through the mail, or a terrorist attack? Automatically parsing and interpreting such information, even with today’s most sophisticated computing tools, is exceptionally difficult. To do so in an automated way, transcribing and data-mining the contents of hundreds of millions of telephone calls per day is an even more difficult task. It is not surprising, then, that intelligence and law enforcement agencies often turn first to metadata. Examining metadata is generally more cost-effective than analyzing content. Of course, the NSA will likely still have analysts listen to every call made by the highest-value surveillance targets, but the resources available to the NSA do not permit it to do this for all of the calls of 300 million Americans.

Surveillance Desirable: Terror—Metadata-Specific [cont'd]

4. Section 215 surveillance helps protect us from terror threats

Carrie F. Cordero, Director, National Security Studies and Adjunct Professor of Law, Georgetown University, Testimony before the Senate Judiciary Committee, 10—2—13, <http://www.judiciary.senate.gov/pdf/10-2-13CorderoTestimony.pdf>, accessed 10-8-13.

Moreover, with respect to 215 in particular and intelligence programs generally, I believe that they should be regularly reviewed and evaluated to determine whether they continue to be necessary and valuable. It is wholly appropriate to end a collection program that has outlived its usefulness, or perhaps is no longer necessary based on new technologies or methods of collecting intelligence that may be more efficient or productive. But, based on what senior leaders of the Intelligence Community are advising today, the 215 program remains a valuable part of the protective infrastructure that was implemented after September 11th. Therefore, in my view, it would be premature for Congress to end it altogether, abruptly through legislation.

5. Metadata analysis is largely impervious to most existing encryption and other masking techniques

Edward W. Felten, Professor, Computer Science and Public Affairs, Princeton University, Testimony before the Senate Intelligence Committee, 10—2—13, <http://www.judiciary.senate.gov/pdf/10-2-13FeltenTestimony.pdf>, accessed 10-8-13.

As a general matter, it is practically impossible for individuals to avoid leaving a metadata trail when engaging in real-time communications, such as telephone calls or Internet voice chats. After decades of research (much of it supported by the U.S. government), there now exist many tools that individuals and organizations can use to protect the confidentiality of their communications content. Smartphone applications are available that let individuals make encrypted telephone calls and send secure text messages. Freely available software can be used to encrypt email messages and instant messages sent between computers, which can frustrate surveillance efforts traditionally performed by intercepting communications as they are transmitted over the Internet. However, most of these secure communication technologies protect only the content of the conversation and do not protect the metadata. Government agents that intercept an encrypted email may not know what was said, but they will be able to learn the email address that sent the message and the address that received it as well as the size of the message and when it was sent. Likewise, Internet metadata can reveal the parties making an encrypted audio call and the time and duration of the call, even if the voice contents of the call are beyond the reach of a wiretap.

6. Metadata has no constitutional protections, is enormously useful in stopping terror attacks

John Yoo, Professor, Law, University of California, Berkeley, “The Terrorist Surveillance Program and the Constitution,” *GEORGE MASON LAW REVIEW* v. 14, 2007, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=975333, accessed 10-2-13.

These privacy concerns are exaggerated. The Supreme Court has found that such information does not receive Fourth Amendment protection because the consumer has already voluntarily turned over the information to a third party. It is not covered by FISA because no electronic interception or surveillance of the calls has occurred. Meanwhile, the data is potentially of enormous use in frustrating al Qaeda plots. If our agents are pointed to members of an al Qaeda sleeper cell by a U.S. phone number found in a captured al Qaeda leader’s cell phone, call pattern analysis would allow the NSA to determine the extent of the network and its activities. It could track the sleeper cell as it periodically changed phone numbers. This could give a quick, initial database-generated glimpse of the possible size and activity level of the cell in an environment where time is of the essence.

7. We need to let law enforcement study patterns to prevent attacks

John Yoo, Professor, Law, University of California, Berkeley, “The Terrorist Surveillance Program and the Constitution,” *GEORGE MASON LAW REVIEW* v. 14, 2007, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=975333, accessed 10-2-13.

At this point it is important to emphasize that no one is being declared guilty of anything—all that might be done at this point is to seek more information, deploy more resources, or seek a warrant. It would be foolhardy to prevent our intelligence and law enforcement officers from studying patterns of private behavior to stop future attacks. Police routinely rely on the study of patterns, analyzing the “m.o.” of past crimes, or patterns of criminal activity in certain neighborhoods at different times, in order to try to predict future crimes. Computerization, though no panacea, could reasonably protect privacy by preventing human eyes from ever seeing the irrelevant records of innocent activity.

Surveillance Desirable: Terror—Metadata-Specific [cont'd]

8. There is not direct surveillance of content and the metadata program is vital to stopping attacks

Marc A. Thiessen, American Enterprise Institute, “Big Brother Isn’t Watching You,” WASHINGTON POST, 6—10—13, <http://aei.org/article/foreign-and-defense-policy/terrorism/big-brother-isnt-watching-you/>, accessed 10-3-13. But instead of being outraged by the damage done by these leaks, critics on the left and right are criticizing the NSA for undertaking activities that are lawful, constitutional and absolutely vital to protecting the country. Calm down, folks. Big Brother is not watching you. During the Bush administration, critics opposed what they called “warrantless wiretapping.” Well, the leaked NSA operations are not warrantless. And, in the case of Verizon, they do not even involve wiretapping. The Verizon court order shows that what is being tracked is not the content of the communications but the records of which phone number called which number, as well as the location and duration of the calls. In *Smith v. Maryland*, the Supreme Court held that there’s no reasonable expectation of privacy, and thus no Fourth Amendment protection, for the phone numbers people dial (as distinct from the content of the call), because the number dialed is information you voluntarily share with the phone company to complete the call and for billing purposes. Why does the NSA need to collect all that data? One former national security official explained it to me this way: If you want to connect the dots and stop the next attack, you need to have a “field of dots.” That is what the NSA is collecting. But it doesn’t dip into that field unless it comes up with a new “dot” — for example, a new terrorist phone number found on a cellphone captured in a raid. It will then plug that new “dot” into the “field of dots” to find out which dots are connected to the new number. If you are not communicating with that terrorist, your dot is not touched. But the NSA needs to have the entire field of dots so it can unravel the network connected to that terrorist. In the case of the PRISM program, the NSA is targeting foreign nationals, not U.S. citizens, and not even individuals in the United States. And all of this collection is being done with a warrant, issued by a federal judge, under authorities approved by Congress.

9. Enhanced data analysis tools are needed to foil terror attacks

Paul Rosenzweig, visiting fellow, Heritage Foundation, Testimony before the Senate Subcommittee on Oversight of Government Management, the Federal Workforce and the District of Columbia Committee on Homeland Security and Governmental Affairs, 7—31—12, <http://www.heritage.org/research/testimony/2012/08/the-state-of-privacy-and-security-our-antique-privacy-rules>, accessed 10-3-13.

Cyberspace is the natural battleground for enhanced analytical tools that are enabled by the technology of data collection. If our goal is to combat terrorists or insurgents (or even other nations) then the cyber domain offers us the capacity not just to steal secret information through espionage, but to take observable public behavior and information and use cyber tools to develop a more nuanced and robust understanding of their tactics and intentions. Likewise, it can be used by our opponents to uncover our own secrets. Traditionally, the concept of “surveillance” has been taken to mean an act of physical surveillance—e.g., following someone around or planting a secret camera in an apartment. As technology improved, our spy agencies and law enforcement institutions increasingly came to rely on even more sophisticated technical means of surveillance, and so we came to develop the capacity to electronically intercept telecommunications and examine email while in transit.

10. Metadata is a powerful intelligence tool—can be used to gain vital insights

Edward W. Felten, Professor, Computer Science and Public Affairs, Princeton University, Testimony before the Senate Intelligence Committee, 10—2—13, <http://www.judiciary.senate.gov/pdf/10-2-13FeltenTestimony.pdf>, accessed 10-8-13. Metadata can now yield startling insights about individuals and groups, particularly when collected in large quantities across the population. It is no longer safe to assume that this “summary” or “non-content” information is less revealing or less sensitive than the content it describes. Just by using new technologies such as smart phones and social media, we leave rich and revealing trails of metadata as we move through daily life. Many details of our lives can be gleaned by examining those trails. Taken together, a group’s metadata can reveal intricacies of social, political, and religious associations. Metadata is naturally organized in a way that lends itself to analysis, and a growing set of computing tools can turn these trails into penetrating insights. Given limited analytical resources, analyzing metadata is often a far more powerful analytical strategy than investigating content: It can yield far more insight with the same amount of effort.

Surveillance Desirable: Terror—Metadata-Specific [cont'd]

11. Data mining is the best way to prevent future terrorist attacks

John Yoo, Professor, Law, University of California, Berkeley, “The Terrorist Surveillance Program and the Constitution,” *GEORGE MASON LAW REVIEW* v. 14, 2007, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=975333, accessed 10-2-13.

Living within FISA’s law enforcement framework will hamper efforts to take advantage of what is known as data mining. Data mining refers to the practice of using powerful supercomputers and advanced algorithms to analyze vast amounts of information for patterns of behavior. In the United States, corporations employ data mining techniques to market products, like credit cards and magazine subscriptions, and to identify likely buyers based on their income level, geographic location, and purchasing and travel histories—as well as to detect fraud. Similarly, financial companies analyze various patterns of behavior to discover suspicious activity that might suggest someone has stolen a credit card or account number. Government data mining theoretically could compile information from government, public, and commercial databases to allow investigators to search for patterns of behavior that might correlate with terrorist activity. Airline security uses a simple variant of this approach when it identifies passengers for extra security screening—a foreign citizen buying a one-way, full-fare ticket, in cash, on the day of the flight would likely trigger a second look from airline security personnel. Data mining is the best hope for an innovative counter-terrorism strategy to detect and prevent future al Qaeda attacks. Rather than hope an agent will one day penetrate al Qaeda’s inner circles—a dubious possibility—or that we will successfully seal our vast borders from terrorists, data mining would allow us to see patterns of activity that reveal the al Qaeda network’s activity before it can attack. Computerized pattern analysis could quickly reveal whether anyone linked to al Qaeda made large purchases of chemicals or equipment that could be used for explosives or chemical weapons. We could learn whether they traveled regularly to certain cities, and we could discover where they stayed and who they called in those cities.

12. Absolute protections against data mining would make it difficult for us to foil some terror attacks

John Yoo, Professor, Law, University of California, Berkeley, “The Terrorist Surveillance Program and the Constitution,” *GEORGE MASON LAW REVIEW* v. 14, 2007, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=975333, accessed 10-2-13.

As civil libertarians complain, almost all transactions of this nature—calling, emailing, spending money, traveling—are innocent. We engage in them every day. That is exactly why al Qaeda has trained its operatives to use them as tools to conceal their plots. Al Qaeda’s leaders understand the difficulty in analyzing billions of transactions and interactions every day to detect their cells, and they realize that western societies impose legal obstacles on government access to such information. Civil libertarian critics don’t seem to have noticed that our government already employs modest forms of data mining to track down criminals and terrorists. In response to drug cartels and organized crime, our government has used simple data mining to track and analyze money flows for years. Banks and financial institutions provide records of financial transactions to the Department of the Treasury, which searches the patterns for money laundering activity. While the great majority of the transactions are legal, the information can piece together proof of criminal links after a conspiracy has been stopped, or it can help indicate suspicious activity that demands further investigation. Analyzing money flows has also proven to be an important tool in detecting and breaking up terrorist networks. If civil libertarians are right, consumers would also have an absolute right to privacy over their banking transactions and our government would lose this valuable, commonsense tool to combat crime, as well as terrorism. Two examples illustrate this point: (1) the NSA’s use of phone records and (2) the Total Information Awareness program.

Surveillance Desirable: Terror—Metadata-Specific [cont'd]

13. Metadata is very easy to analyze

Edward W. Felten, Professor, Computer Science and Public Affairs, Princeton University, Testimony before the Senate Intelligence Committee, 10—2—13, <http://www.judiciary.senate.gov/pdf/10-2-13FeltenTestimony.pdf>, accessed 10-8-13. Telephony metadata is easy to aggregate and analyze because it is, by its nature, structured data. Telephone numbers are standardized, and are expressed in a predictable format: in the United States, a three digit area code, followed by a three digit central office exchange code, and then a four digit subscriber number. Likewise, the time and date information associated with the beginning and end of each call will be stored in a predictable, standardized format. By contrast, the contents of calls are unstructured. Some people speak English, others Spanish, French, Mandarin, or Arabic. Some speak using street slang or a pidgin dialect, which can be difficult for others to understand. Conversations lack a common structure: Some people get straight to the point, others engage in lengthy small talk. Speakers have different accents, and exhibit verbal stutters and disfluencies. Although automated transcription of speech has advanced, it is still a difficult and error-prone process. The structured nature of metadata makes it easy to analyze massive datasets using sophisticated data-mining and link-analysis programs. That analysis is greatly facilitated by technological advances over the past decades in computing, electronic data storage, and digital data mining. Those advances have radically increased our ability to collect, store, and analyze personal communications, including metadata. Further, the massive increases in electronic storage permit us to maintain, cheaply and efficiently, vast amounts of data. The ability to preserve data on this scale is, by itself, an unprecedented development—making possible the maintenance of a digital history that was not previously within the easy reach of any individual, corporation, or government.

14. The NSA programs are necessary to stop terrorist attacks

Marshall Curtis Erwin, and Edward C. Liu, Congressional Research Service, “NSA Surveillance Leaks: Background and Issues for Congress,” CRS REPORT FOR CONGRESS, 7—2—13, p. 10.

The Administration has argued that the surveillance activities leaked to the press, in addition to being subject to oversight by all three branches of government, are important to national security and have helped disrupt terror plots. These arguments have not always distinguished between the two programs, but generally the Administration appears to have taken the position that collection pursuant to Section 702 is an important tool on a broad range of national security issues and that collection pursuant to Section 215 has been useful in a discrete number of terrorism cases. Regarding bulk phone records, which have come under greater scrutiny, intelligence officials have argued that the breadth of the collection is necessary to ensure all relevant information is available to the government and can be identified through searches in NSA’s database, rather than having more focused collection that might miss relevant information. For example, Deputy Attorney General James Cole before the HPSCI stated “if you’re looking for a needle in the haystack, you have to get the haystack first.”

Surveillance Desirable: Terror—Presidential Flexibility Key

1. Presidential flexibility is necessary to prevent WMD terror attacks

John Yoo, Professor, Law, University of California, Berkeley, “The Terrorist Surveillance Program and the Constitution,” *GEORGE MASON LAW REVIEW* v. 14, 2007, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=975333, accessed 10-2-13.

Legislative deliberation can breed consensus in the best of cases, but it also can stand in the way of speed and decisiveness. Terrorist attacks are more difficult to detect and prevent than those posed by conventional armed forces and nations, and WMDs allow terrorists to inflict devastation that once only could have been achievable by a nation-state. To defend itself from this threat, the United States will have to use force earlier and more often than at the time when nations generated the primary threats. In order to forestall a WMD attack, or to take advantage of a window of opportunity to strike at a terrorist cell, the President needs the flexibility to act quickly. By acting earlier, perhaps before WMD components have been fully assembled or before an al Qaeda operative has left for the United States, the executive branch might also be able to engage in a more limited, more precisely targeted, use of force.

2. Placing Congress in charge discourages innovation and increases terrorism threats

John Yoo, Professor, Law, University of California, Berkeley, “The Terrorist Surveillance Program and the Constitution,” *GEORGE MASON LAW REVIEW* v. 14, 2007, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=975333, accessed 10-2-13.

Critics of the NSA program want to overturn American historical practice in favor of a new and untested theory about the wartime powers of the President and Congress. We should encourage innovation and creativity in our intelligence and military—and the NSA program is precisely that—to confront the unprecedented challenges of al Qaeda. For too long, our system retarded aggressive measures to pre-empt terrorist attacks. But seeking to give Congress the dominant hand in setting wartime policy would render our tactics against al Qaeda less, rather than more effective. It would slow down decisions, make sensitive policies and intelligence public, and encourage risk aversion rather than risk taking. It ignores the reality of the al Qaeda challenge to require the President to seek, every time he wants to make an important policy change, congressional permission first.

3. The President should have flexibility in using tools like the NSA to prevent attacks

John Yoo, Professor, Law, University of California, Berkeley, “The Terrorist Surveillance Program and the Constitution,” *GEORGE MASON LAW REVIEW* v. 14, 2007, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=975333, accessed 10-2-13.

The Constitution creates a presidency whose function is to act forcefully and independently to repel serious threats to the nation. Instead of specifying a legalistic process to begin war, the framers wisely created a fluid political process in which legislators would use their funding, legislative, and political power to balance presidential initiative. As we confront terrorism, potentially armed with weapons of mass destruction, we should look skeptically at claims that radical changes in the way we make war would solve our problems, even those stemming from poor judgment, unforeseen circumstances, and bad luck. The worst thing we could do when confronted by a capable, shadowy enemy like al Qaeda would be to change our government to make it harder to develop innovative policies like the NSA surveillance program.

Surveillance Desirable: Terror—PRISM-Specific

- Programs like PRISM protect us against terrorist attacks

James Jay Carafano, Vice President for Defense and Foreign Policy studies, Heritage Foundation, "PRISM Is Essential to U.S. Security in War Against Terrorism," WASHINGTON EXAMINER, 8—6—13, <http://www.heritage.org/research/commentary/2013/8/prism-is-essential-to-us-security-in-war-against-terrorism>, accessed 10-4-13.

Congress has not been much better. The authority for PRISM is in FISA Section 702. Congress debated these authorities in 2007 and again when the program was reauthorized in 2008. Senate Majority Leader Harry Reid, D-Nev., surely remembers the controversy. He wrote President Bush: "There is no crisis that should lead you to cancel your trip to Africa. But whether or not you cancel your trip, Democrats stand ready to negotiate a final bill, and we remain willing to extend existing law for as short a time or as long a time as is needed to complete work on such a bill." Evidently, Reid must have felt the authorities granted under Section 702 received a full and sufficient hearing. Most current members of Congress were seated under the dome during the 2008 debates. They had every opportunity not just to read the law, but to be briefed on the program by intelligence officials before voting on the bill. For them to act shocked at the scope of the program today rings about as hollow as Obama's expressed disdain for the operations he oversees. The reality is that Congress and the administration share responsibility for these programs. If they want to change or modify them, who's stopping them? If changes are made, however, they should to be made for the right reason. Leaders must never compromise our security for political expediency. At least 60 Islamist-inspired terrorist plots have been aimed at the U.S. since the 9/11 attacks. The overwhelming majority have been thwarted thanks to timely, operational intelligence about the threats. Congress should not go back to a pre-/11 set of rules just to appeal to populist sentiment. Congress and the White House have an obligation to protect our liberties and to safeguard our security -- in equal measure. Meeting that mission is more important than winning popularity polls.

Surveillance Desirable: Terror Threat—Al Qaeda

1. The threat posed by Al Qaeda is real—authoritative U.N. report proves

Jason Burke, "Al-Qaida Remains Significant Threat to West—UN Report," GUARDIAN, 8—7—13, www.theguardian.com/world/2013/aug/07/al-qaida-threat-west-un, accessed 10-2-13.

Al-Qaida remains a significant threat to western targets as it "continues to diversify" into increasingly self-radicalised extremist groups, despite significant damage to its "core" leadership, according to an authoritative new United Nations report. The report, to be released later on Wednesday, describes the threat posed by al-Qaida as made up of "loosely linked affiliates", with self-radicalised terrorists influenced by an "infectious" ideology flourish. The analysis comes amid an increasingly acrimonious and politicised debate about the relative success or failure of strategies pursued by the US and allied nations to counter the organisation in recent years. White House spokesman Jay Carney on Tuesday called al-Qaida "severely diminished" and "decimated." President Barack Obama, who ordered the May 2011 raid that killed Osama bin Laden, has described al-Qaida's headquarters as "a shadow of its former self". However, this week critics have pointed out that the US administration has been forced to close 19 diplomatic outposts stretching across the Middle East, Africa and Asia, and evacuate nonessential personnel from the US embassy in Yemen. The UK has also evacuated staff from Yemen. The new report, the 14th issued by analysts working for the Security Council Committee which deals with sanctions on al-Qaida "and associated individuals and entities", is seen as non-partisan and rigorous. It draws on intelligence inputs from all member nations of the UN and academic work. "While the threat posed by al-Qaida as a global terrorist organisation has declined, the threat posed by its affiliates and its infectious ideas persists," it says. One key question for analysts has been the influence of the remnant of al-Qaida's senior leadership based in Pakistan's restive western zones. Here the report is unequivocal. "Al-Qaida's core has seen no revival of its fortunes over the past six months. A degraded senior leadership based in the Afghanistan-Pakistan border region continues to issue statements, but demonstrates little ability to direct operations through centralised command and control," it says.

2. Al Qaeda's message continues to resonate even as we make progress in killing the leadership

Jason Burke, "Al-Qaida Remains Significant Threat to West—UN Report," GUARDIAN, 8—7—13, www.theguardian.com/world/2013/aug/07/al-qaida-threat-west-un, accessed 10-2-13.

Yet, the report points out, "the reality of al-Qaida's diminished capabilities and limited appeal does not mean that the threat of al-Qaida attacks has passed" as "individuals and cells associated with al-Qaida and its affiliates continue to innovate with regard to targets, tactics and technology." The threat is changing however as terrorist propaganda on the Internet continues to grow in sophistication and reach, contributing to the problem of self-radicalisation. Recent attacks, such as that in Boston in April perpetrated by two Chechen brothers living in the US with no known link to al-Qaida, "point to the persistent challenge of acts of expressive terrorist violence committed by individuals or small groups." These, the reports says, are "troubling" as they "may draw on autonomous attack plans rather than the specific leadership tasking of either al-Qaida or affiliates." Finally, the continuing civil war in the Syrian Arab Republic has seen the emergence of a strong al-Qaida presence drawing from al-Qaida in Iraq attracting hundreds of recruits from outside the Syrian Arab Republic. A new communiqué from al-Zawahiri, who as early as December 2001 announced plans to decentralise the network and scatter its affiliates across the globe as a way of ensuring its survival. "Even while the core al-Qaida group may be in decline, al-Qaida-ism, the movement's ideology, continues to resonate and attract new adherents," Bruce Hoffman, director of the Security Studies Program at Georgetown University, wrote in a research paper earlier this year. Bin Laden's death, Hoffman wrote, "left behind a resilient movement that, although seriously weakened, has been expanding and consolidating its control in new and far-flung locales."

3. Al Qaeda remains a threat

Marc Thiessen, "Why We Need NSA Surveillance: RAND Study Finds Al Qaeda Expanding," AEI IDEAS, American Enterprise Institute, 7—23—13, www.aei-ideas.org/2013/07/why-we-need-nsa-surveillance-rand-study-finds-al-qaeda-expanding/, accessed 10-2-13.

The Christian Science Monitor reports: Al Qaeda not only remains a threat to the United States, but its capabilities and scope are expanding, a new analysis from a respected think tank has concluded. "There has been a net expansion in the number and geographic scope of Al Qaeda affiliates and allies over the past decade, indicating that Al Qaeda and its brand are far from defeated," argues Seth Jones, an analyst at the RAND Corporation and the study's author.

Surveillance Desirable: Terror Threat—Al Qaeda [cont'd]

4. Al Qaeda remains a threat—splinter groups

Rowan Scarborough, “Al Qaeda Remains a Threat to U.S. Via Its Franchises Despite Obama’s Boast,” WASHINGTON TIMES, 5—29—13, www.washingtontimes.com/news/2013/may/29/al-qaeda-still-threat-despite-obamas-claim/?page=all, accessed 10-2-13.

Terrorism analysts say that as the U.S. conducted a concentrated air war via armed Predators against al Qaeda’s core leadership in Pakistan’s tribal areas for more than a decade, the group’s Islamic chieftains decided to diversify. “I totally disagree with the premise that al Qaeda is on the path to defeat,” said retired Army Gen. Jack Keane, who has advised U.S. commanders in the Iraq and Afghanistan wars. “Quite the contrary, al Qaeda has deliberately decentralized its operations, not because of the relentless attacks we have had on its national leadership in Pakistan, but because its strategic objective is to dominate and control Muslim countries in the region. As such, al Qaeda must extend its geographic reach, which is not only successful but is expanding.” Three al Qaeda franchises are most notable: al Qaeda in Iraq, which has rebuilt and stepped up attacks since the last American troops left in 2011 and has moved fighters into Syria; al Qaeda in the Islamic Maghreb (AQIM), a North Africa-based network aligned with Ansar al Shariah, which carried out the deadly assault on the U.S. diplomatic mission in Benghazi, Libya; and al Qaeda in the Arabian Peninsula (AQAP), a Yemen-based cell that sponsored the failed 2009 airliner attack by “underwear bomber” Umar Farouk Abdulmutallab. Gen. Keane’s assertions that al Qaeda remains powerful seems to be supported by administration witnesses earlier this year. “The threat from AQAP, particularly with airliners, has not dissipated over the years,” FBI Director Robert S. Mueller III told the Senate Select Committee on Intelligence. “There’s still that threat out there. The individuals who were responsible for the previous attempts are still there.” Matthew Olsen, who heads the National Counterterrorism Center, said al Qaeda is still trying to recruit attackers in the United States. “We definitely have seen, both from the al Qaeda core in Pakistan as well as AQAP in Yemen, an effort to reach out beyond those regions into the United States to radicalize individuals who are here, who may be susceptible to that kind of a message,” Mr. Olsen testified. “They may be simply wayward knuckleheads, but they may well be inspired by that message and seek to carry out an attack.” Retired Marine Gen. James N. Mattis, in his final testimony to the House Armed Services Committee as head of U.S. Central Command, called al Qaeda “a real threat.” Navy Adm. William H. McRaven, who directs U.S. Special Operations Command, which targets individual terrorists and cells, testified that it is not enough to target a single al Qaeda group because the network establishes alliances with like-minded Islamic extremists. He explained the challenge in just one part of the world: North Africa. “I certainly think we understand the complexity of the al Qaeda network,” he said in Senate testimony. “And if you look in Africa as an example, you have al Qaeda in the Islamic Lands of the Maghreb, and we know that they are partnered or linked with Boko Haram out of Nigeria. So you certainly cannot isolate a single organization, whether it’s al Qaeda in the Islamic Lands of the Maghreb or Boko Haram, and expect to be able to solve the problem either locally by going after that problem in a particular country or by individual entity. If you deal with AQIM, you probably have to deal with Boko Haram.”

5. Al Qaeda is expanding and remains a serious threat

Rowan Scarborough, “Al Qaeda Remains a Threat to U.S. Via Its Franchises Despite Obama’s Boast,” WASHINGTON TIMES, 5—29—13, www.washingtontimes.com/news/2013/may/29/al-qaeda-still-threat-despite-obamas-claim/?page=all, accessed 10-2-13.

According to a Heritage Foundation study, Islamists have plotted 54 times to strike American since Sept. 11, 2001, the day al Qaeda operatives flew airplanes into the World Trade Center and Pentagon. Three other plots were carried out, the most recent the Boston Marathon bombings. CIA Director John O. Brennan, Mr. Obama’s former counterterrorism adviser, seemed to paint a more dangerous picture of al Qaeda during his Senate confirmation hearing than the president did during his recent speech. “We remain at war with al Qaeda and its associated forces, which despite the substantial progress we have made against them, still seek to carry out deadly strikes against our homeland, our citizens and against our friends and allies,” Mr. Brennan said. He conceded that, rather than pulling back, al Qaeda is expanding: “I will say that if you look out over the last four years, what happened in a number of places, such as Yemen and other areas, where there was in fact a growth of al Qaeda, quite unfortunately.” Gen. Keane said that while al Qaeda’s core has been badly damaged by the loss of senior leaders, including Osama bin Laden, it has established itself in other countries where it did not exist on Sept. 11, 2001. He listed the countries — Libya, Syria, Iraq, Somalia, Mali, Yemen — where al Qaeda spinoffs are growing. “Al Qaeda has returned to Iraq after it was defeated in 2009, is the fastest growing rebel group in Syria, has established a bona fide sanctuary in [the West African nation of] Mali and attempted to seize the capital, and established a clear sanctuary in eastern Libya where no actions have been taken against the al Qaeda affiliated group, Ansar al-Shariah,” the retired general said. “In Somalia, we have enjoyed some success, and in Yemen it’s at best a draw.”

Surveillance Desirable: Terror Threat—Al Qaeda [cont'd]

6. Al Qaeda will coordinate with other groups to fill any capabilities gaps to use a nuclear weapons

Matthew Bunn, Associate Professor, Public Policy, Harvard University, Colonel Yuri Morozov, Professor, Russian Academy of Military Sciences, Rolf Mowatt Larssen, Senior Fellow, Harvard University, Simon Saradzhyan, Fellow, Harvard University, William Tobey, Senior Fellow, Harvard University, Viktor I.L.Yesin, Senior Fellow, Russian Academy of Sciences, and Pavel S. Zolotarev, Deputy Director, U.S.A. and Canadian Institute, Russian Academy of Sciences, THE U.S.-RUSSIA JOINT THREAT ASSESSMENT ON NUCLEAR TERRORISM, 5--11, p. 32.

Overcoming the formidable obstacles in planning a nuclear attack would be facilitated by the collaboration of like-minded groups. Al-Qaeda has a history of working with other groups on WMD. Ayman al-Zawahiri solicited the assistance of JI leader Riduan Isamuddin (also known as Hambali) to help create a Southwest Asian-based anthrax network, which was led by hard-core JI operative Yazid Sufaat. This network complemented al-Qaeda's Pakistan-based anthrax network, which was led by a mid-level government biologist named Rauf Ahmed. Al-Zawahiri personally supervised the two networks, keeping them separate and independent of each other. He personally tasked each group with somewhat redundant missions in pursuit of a single objective: the development of a lethal strain of anthrax capable of producing mass casualties and economic damage. Al-Zawahiri's tradecraft in recruiting and handling the operatives in these two networks was well-disciplined and fairly effective, although it appears that the roughly two-year project was abandoned in the summer before 9/11, probably without reaching fruition. Due to the fact that planning is being directed by the same narrow circle of people, the methodology of the al-Qaeda leadership's nuclear efforts is likely to share certain similarities with the anthrax project. While assessing al-Qaeda's options in acquiring nuclear-related capabilities, the possibility must be taken into account that the al-Qaeda core might consider joining forces with senior leaders of North Caucasus terrorists, and groups like Lashkar al-Tayyib, in a joint effort to acquire a nuclear bomb.

Surveillance Desirable: Terror Threat—Bioterrorism

1. The effects of a successful bioterror attack are incalculable

Anders Sandberg et al., James Martin Research Fellow, Future of Humanity Institute, Oxford University, "How Can We Reduce the Risk of Human Extinction?" BULLETIN OF THE ATOMIC SCIENTISTS, 9—9—08, <http://www.thebulletin.org/web-edition/features/how-can-we-reduce-the-risk-of-human-extinction>, accessed 10-3-13.

The risks from anthropogenic hazards appear at present larger than those from natural ones. Although great progress has been made in reducing the number of nuclear weapons in the world, humanity is still threatened by the possibility of a global thermonuclear war and a resulting nuclear winter. We may face even greater risks from emerging technologies. Advances in synthetic biology might make it possible to engineer pathogens capable of extinction-level pandemics. The knowledge, equipment, and materials needed to engineer pathogens are more accessible than those needed to build nuclear weapons. And unlike other weapons, pathogens are self-replicating, allowing a small arsenal to become exponentially destructive. Pathogens have been implicated in the extinctions of many wild species. Although most pandemics "fade out" by reducing the density of susceptible populations, pathogens with wide host ranges in multiple species can reach even isolated individuals. The intentional or unintentional release of engineered pathogens with high transmissibility, latency, and lethality might be capable of causing human extinction. While such an event seems unlikely today, the likelihood may increase as biotechnologies continue to improve at a rate rivaling Moore's Law.

2. Bioweapons outweigh—spread much more, threaten the entire global population

Rita Grossman-Vermaas, Brian D. Finlay, and Elizabeth Turpen, Ph.D., OLD PLAGUES, NEW THREATS: THE BIOTECH REVOLUTION AND ITS IMPACT ON U.S. NATIONAL SECURITY, Henry L. Stimson Center, March 2008, p. 1.

For decades, national security and law enforcement communities in our country, and in countries around the globe, have worked diligently to address the threat posed by the deliberate spread of infectious pathogens and deadly toxins. As potential agents of mass destruction, biological pathogens and toxins are inexpensive, readily accessible in nature, and, if weaponized effectively, particularly dangerous. Meanwhile, the biotechnological revolution has broadened the availability of "dual-use" equipment and expanded exponentially the number of individuals with the knowledge necessary to engage in nefarious biological weapons research. Although biological weapons are often put in the same category as nuclear and chemical munitions by national security specialists, there is one fundamental and important difference: pathogens are living organisms. The implications of this are clear. While the damage caused by a chemical or nuclear weapon would be a single event causing potentially devastating damage over the immediate site of its target, the release of a lethal pathogen could efficiently spread from victim to victim over time, creating a cascade of disease that could threaten the entire global population.

3. Even small attacks wreck the economy—trillions in losses

NUCLEAR NEWS, "The Clock is Ticking on Taking Preventive Action," December 2009, npg.

The report also says that the threat of bioterrorism is real. In its December 2008 report, "World at Risk," the commission concluded that terrorists are more likely to be able to obtain and use a biological weapon than a nuclear weapon, and in recent years the United States has received strategic warnings of biological weapons use from dozens of government reports and expert panels. The consequences of ignoring these warnings could be dire, according to the October report. For example, the report notes that "one recent study from the intelligence community projected that a one- to two-kilogram release of anthrax spores from a crop duster plane could kill more Americans than died in World War II. Cleanup and other economic costs could exceed \$1.8 trillion."

4. Bioattack impact incalculable—killed hundreds of millions in the past, could be worse now

Timothy K. Gilman, JD Candidate, Georgetown University, "Search, Sentence and (Don't) Sell; Combating the Threat of Biological weapons Through Inspections, Criminalization, and Restrictions on Equipment," JOURNAL OF TRANSNATIONAL LAW & POLICY v. 12, Spring 2003, p. 217+.

Biological weapons represent a significant threat to the security and health of the United States and the rest of the world. Naturally occurring biological agents, such as smallpox, have been responsible for hundreds of millions of deaths over the last century. Advances in biotechnology have created the potential to make these agents even more dangerous. The potential damage from a large-scale attack using sophisticated bioweapons is incalculable.

Surveillance Desirable: Terror Threat—Nuclear Terrorism

1. A single successful nuclear terror strike would crush global trade

William Tobey, senior fellow, Belfer Center for International Affairs, Harvard University, Testimony before the Canadian Special Senate Committee on Anti-Terrorism, 6--11--12, http://belfercenter.ksg.harvard.edu/publication/22127/special_senate_committee_on_antiterrorism.html?breadcrumb=%2Fexperiments%2F368%2Fmatthew_bunn, accessed 4-4-13.

One can only imagine the devastating consequences should a terrorist group succeed in detonating a nuclear weapon in a major city. Tens -- perhaps hundreds -- of thousands of people might be killed or injured. International commerce might grind to a halt as border control authorities struggled to ensure that no such devices entered other countries. Of course, international security arrangements would be changed in ways far more profound than the sweeping changes caused by the September 11 attacks.

2. Impact is so large that we must act to stop it--terrorists want a nuke, can obtain and use one

Matthew Bunn, Associate Professor, Public Policy, Harvard University, Colonel Yuri Morozov, Professor, Russian Academy of Military Sciences, Rolf Mowatt Larssen, Senior Fellow, Harvard University, Simon Saradzhyan, Fellow, Harvard University, William Tobey, Senior Fellow, Harvard University, Viktor I. Yesin, Senior Fellow, Russian Academy of Sciences, and Pavel S. Zolotarev, Deputy Director, U.S.A. and Canadian Institute, Russian Academy of Sciences, THE U.S.-RUSSIA JOINT THREAT ASSESSMENT ON NUCLEAR TERRORISM, 5--11, p. 3.

Nuclear terrorism is a real and urgent threat. Given the potentially catastrophic consequences, even a small probability of terrorists getting and detonating a nuclear bomb is enough to justify urgent action to reduce the risk. Al-Qaeda and North Caucasus terrorist groups have both made statements indicating that they seek nuclear weapons and have attempted to acquire them; these groups are presented together as a case study to assess nuclear terrorism as a present and future threat. (The only other terrorist group known to have systematically sought to get nuclear weapons was the Japanese cult group Aum Shinrikyo.) This study makes the case that it is plausible that a technically sophisticated group could make, deliver, and detonate a crude nuclear bomb if it could obtain sufficient fissile material.

3. Nuclear terror wrecks the economy—fear of follow on attacks causes widespread panic

Matthew Bunn, Associate Professor, Public Policy, Kennedy School of Government, Harvard University, SECURING THE BOMB 2010, April 2010, p. 3-6.

It is important to understand the full history-changing scope of the catastrophe that even a single terrorist nuclear bomb could cause. The heart of a major city could be reduced to a smoldering radioactive ruin, leaving tens or hundreds of thousands of people dead. Terrorists—either those who committed the attack or others—would probably claim they had more bombs already hidden in other cities (whether they did or not), and the fear that this might be true could lead to panicked evacuations, creating widespread havoc and economic disruption. Some countries may feel that nuclear terrorism is really only a concern for the countries most likely to be the targets, such as the United States. In reality, however, such an event would cause devastating economic aftershocks worldwide. In 2005 then-UN Secretary-General Kofi Annan warned that these global effects would push “tens of millions of people into dire poverty,” creating “a second death toll throughout the developing world.”

Surveillance Desirable: Terror Threat—Answers to “Bioterror Unlikely”

1. Bioterror attack is more likely--easy to weaponize, obtain materials, "reload" and attack again

Bob Graham and Jim Talent, chairs, Commission on the prevention of Weapons of Mass Destruction Proliferation and Terrorism, Testimony before the House Committee on Homeland Security, 4—21—10, <http://www.heritage.org/Research/Testimony/Hearing-on-the-Weapons-of-Mass-Destruction-Prevention-and-Preparedness-Act-of-2010>, accessed 10-3-13..

The Commission's Report assessed both nuclear and biological threats, and provided 13 recommendations and 49 action items. The Commissioners unanimously concluded that unless we act urgently and decisively, it was more likely than not that terrorists would attack a major city somewhere in the world with a weapon of mass destruction by 2013. Furthermore, we determined that terrorists are more likely to obtain and use a biological weapon than a nuclear weapon. Shortly thereafter, this conclusion was publicly affirmed by then Director of National Intelligence (DNI) Mike McConnell. There are several reasons for our conclusion that a bioattack is actually more likely than a nuclear attack. Many pathogens suitable for use in a biological attack are found in the natural environment, all over the globe. The lethality of an effectively dispersed biological weapon could rival or exceed that of an improvised nuclear device. The equipment required to produce a large quantity from a small seed stock, and then "weaponize" the material--that is, to make it into a form that could be effectively dispersed--is of a dual-use nature and readily available on the Internet. The most effective delivery methods are well known in the pharmaceutical, agricultural, and insect-control industries. It is much more straightforward to stockpile weaponized pathogens than nuclear material, raising the terrible specter that terrorists could attack an American city using a bioweapon, then quickly "reload" and attack again within a matter of days or weeks. So, while it is certainly possible for terrorist groups to get a nuclear weapon, it is less difficult for them to develop and disperse a bio-weapon. There may be even fewer barriers for terrorist groups with close ties to those nation states which are accumulating both the materials and scientific capability for weaponization. All of the ingredients are in place for a biological weapon to be in the hands of a terrorist organization, which is subject to none of the international law constraints and retaliatory consequences which might impede a nation state from its use. None of this is speculation. Al-Qaeda was well down the road to producing such weapons prior to 9/11. Due to the ease in creating a clandestine production capability, our intelligence community had no knowledge of two such facilities in Afghanistan prior to their capture by U.S. troops and a separate, but parallel bioweapons development program al-Qaeda ran in Malaysia. Facilities with more sophisticated equipment than those found could be in operation today without our knowledge.

2. Dual use biotech is spreading rapidly, H1N1 virus proves the threat is real

Commission on the Prevention of Weapons of Mass Destruction Proliferation and Terrorism (WMD Commission), PREVENTION OF WMD PROLIFERATION AND TERRORISM REPORT CARD, 1—10, p. 1.

The evolution of the nature of the threat is nowhere more pronounced than in the area of biological weapons. A revolution in biotechnology continues, expanding potentially dangerous dual-use capabilities across the globe. As the delayed response to H1N1 has demonstrated, the United States is woefully behind in its capability to rapidly produce vaccines and therapeutics, essential steps for adequately responding to a biological threat, whether natural or man-made. H1N1 came with months of warning. But even with time to prepare, the epidemic peaked before most Americans had access to vaccine. A bioattack will come with no such warning. Response is a complex series of links in a chain of resilience necessary to protect the United States from biological attacks. Rapid detection and diagnosis capabilities are the first links, followed by providing actionable information to federal, state, and local leaders and the general public; having adequate supplies of appropriate medical countermeasures; quickly distributing those countermeasures; treating and isolating the sick in medical facilities; protecting the well through vaccines and prophylactic medications; and in certain cases, such as anthrax, environmental cleanup. We conclude that virtually all links are weak, and require the highest priority of attention from the Administration and Congress.

3. Threat of biological terror attack is high, growing

Alex Kingsbury, "Slew of Warnings on Nuclear, Biological Terrorism Prompt Worries of Fearmongering," USNEWS.COM, 12—3—08, lexis.

The drumbeat started last month, when Director of National Intelligence Mike McConnell said that the potential for a WMD attack in the coming decades is growing. The probability is increasing, he said, that the world will see "large casualty terrorist attacks using chemical, biological, or, less likely, nuclear materials." And the U.S. intelligence community recently released a study warning of an increased risk of the use of mass-casualty weapons by 2025. Homeland Security Secretary Michael Chertoff echoed the WMD Commission's findings this week, telling reporters that the country is entering "a period of greater strategic threat."

Surveillance Desirable: Terror Threat—Answers to “Bin Laden Death Solves Threat”

1. Terror threat is real—bin Laden’s death is irrelevant

Max Boot, “Bin Laden Is Gone, But Al-Qaeda Is Not,” COMMENTARY, 5—1—12,

www.commentarymagazine.com/2012/05/01/bin-laden-gone-but-al-qaeda-is-not/, accessed 10-3-13.

Al-Qaeda “central” was already in decline prior to its leaders’ death, but as RAND political scientist Seth Jones rightly warns, al-Qaeda remains a very real threat. Especially potent are its regional affiliates (al-Qaeda in the Arabian Peninsula, al-Qaeda in Iraq, al-Qaeda in the Islamic Maghreb) and closely related terrorist organizations such as the Shabaab in Somalia, Boko Haram in Nigeria, and, in Pakistan, Lashkar e Taiba, the Pakistani Taliban, the Afghan Taliban, the Haqqani Network, and others. And that’s not even to mention Hezbollah and Hamas, which in some ways remain the most potent Islamist terrorist organizations of all because they control actual territory. Oh, and in Iraq there is still a threat from various Mahdist army offshoots sponsored by the Iranian Revolutionary Guard’s Quds Force, which has terrorist tentacles stretching all the way from Latin America to the Levant. Faced with this panoply of threats, we would be guilty of wishful thinking if we were to declare victory prematurely. Unfortunately, Islamist-inspired terrorists will continue to threaten our interests—and our homeland—for the foreseeable future. And it is not hard to sketch out possible scenarios—involving, say, a state collapse in Pakistan, a Taliban takeover in Afghanistan, or an Islamist seizure of power in Yemen or Somalia, or the acquisition of WMD by any terrorist group—that could substantially heighten the threat.

2. Al Qaeda is still a threat despite bin Laden’s death

Paul Cruickshank et al., “How Safe Is the Cargo on Passenger Flights?” CNN, 2—19—12,

<http://www.cnn.com/2012/02/16/travel/cargo-terror-concerns/index.html>, accessed 10-3-13.

Despite last year’s elimination of al Qaeda chief Osama bin Laden, the threat from the terrorist group still remains a major concern. Recent months have seen AQAP, the group responsible for the 2010 printer bomb plot, take advantage of political turmoil in Yemen to expand its operations. Saudi Arabia’s counterterrorism service believes this will bolster the group’s ability to target the United States. And it believes Ibrahim al Asiri, the group’s master bomb-maker, has trained several apprentices in how to make sophisticated PETN-based bombs. Markey says that time is not on the United States’ side. “Every day that goes by is another day that al Qaeda might exploit that opening -- and once again successfully terrorize our country,” he told CNN.

3. Terror threat remains—bin Laden’s death does not change that

Christopher Dickey, “The Next Terror Threat,” DAILY BEAST, 5—6—11,

<http://www.thedailybeast.com/articles/2011/05/06/al-qaeda-terror-threat-to-new-york-city-and-us-trains-remains-high.html>, accessed 10-3-13.

Unfortunately, those who follow the terrorist threat most closely don’t think bin Laden’s death will have reduced it much, if at all. “It’s good that we got him,” a senior law enforcement official told me the morning the news broke. “Until we did this, we appeared weak and anemic. But when it comes to terrorism, I don’t think it makes a difference whether he’s alive or not. He wasn’t responsible for Marrakesh. He wasn’t responsible for the guys picked up in Germany on Friday,” the official said, referring to the bombing at a favorite tourist destination in Morocco that killed 16 people last week and the arrest of three men in Germany for allegedly plotting to bomb targets there. Whatever plans bin Laden laid in his Pakistani bedroom, so many al Qaeda sub-groups have sprung up with vicious and ambitious leaders out to prove that they can kill Westerners, too, that the man to whom many supposedly pledged allegiance in fact exercised little or no control over them. The wannabe bin Ladens have already shown they’ll take any shot they can get. They’ve even claimed credit for close calls that failed. As Robert Fisk wrote earlier this week in *The Independent*, the al Qaeda “movement has no ‘leadership’ as such, bin Laden being the founder rather than the boss.” In the end, he had become no more nor less than a symbol himself.

4. Homegrown terror threat is real and growing—bin Laden’s death does not change that

James Carafano, Heritage Foundation, “Bin Laden Dead but Homegrown Terror Threat Remains,” SECURITY DEBRIEF, 5—2—12, <http://securitydebrief.com/2012/05/02/bin-laden-dead-but-homegrown-terror-threat-remains/>, accessed 10-3-13.

It has been almost a year since the death of Osama bin Laden. Though we are right to be proud in dispensing justice to the terrorist mastermind, it is no time to rest on our laurels. Al-Qaeda is weakened and scattered, but this has only led them to adjust their tactics. Al-Qaeda has increasingly reached out to affiliates in the Northern Caucasus and Africa. A particularly worrisome trend is al-Qaeda’s shift toward recruiting homegrown terrorists. Homegrown terrorists can more easily travel to and from the United States without drawing suspicion and have the ability to culturally and linguistically blend into the United States, making the search for such individuals more difficult. A recently released report from the Heritage Foundation indicates that 50 terrorist plots have been foiled since 9/11. Of these 50 foiled plots, 42 were led by individuals who were radicalized right here in the United States. We should be vigilant as we approach the one year anniversary of bin Laden’s death and remember that the threat of terrorism remains very real.

Surveillance Desirable: Terror Threat—Answers to “Border Security”

1. Materials are very difficult to detect

William Tobey, senior fellow, Belfer Center for International Affairs, Harvard University, Testimony before the Canadian Special Senate Committee on Anti-Terrorism, 6--11--12, http://belfercenter.ksg.harvard.edu/publication/22127/special_senate_committee_on_antiterrorism.html?breadcrumb=%2Fexperts%2F368%2Fmatthew_bunn, accessed 4-4-13.

The joint threat assessment concludes that the threat of nuclear terrorism is urgent and real. Making a crude bomb would not be easy, but it is potentially within the capabilities of a technically sophisticated terrorist group if it were to obtain sufficient fissile material or an intact weapon. Al Qaeda has sought nuclear weapons for almost two decades, as have other groups at other times. I would note parenthetically that, given the death of Osama bin Laden, while al Qaeda's capabilities have been blunted, it has not yet been defeated. The nuclear material sufficient for a bomb is small and difficult to detect, making it a major challenge to stop nuclear smuggling or to recover nuclear material after it has been stolen. Hence, the primary focus in reducing the risk of nuclear terrorism must be to keep weapons and fissile material from being stolen by continually improving security.

2. Screening cannot prevent a bomb from being smuggled into the U.S.

Matthew Bunn, Associate Professor, Public Policy, Harvard University, Colonel Yuri Morozov, Professor, Russian Academy of Military Sciences, Rolf Mowatt Larssen, Senior Fellow, Harvard University, Simon Saradzhyan, Fellow, Harvard University, William Tobey, Senior Fellow, Harvard University, Viktor I. Yesin, Senior Fellow, Russian Academy of Sciences, and Pavel S. Zolotarev, Deputy Director, U.S.A. and Canadian Institute, Russian Academy of Sciences, THE U.S.-RUSSIA JOINT THREAT ASSESSMENT ON NUCLEAR TERRORISM, 5--11, p. 10.

The nuclear material for a bomb is small and difficult to detect, making it a major challenge to stop nuclear smuggling, or to recover nuclear material after it has been stolen. Hence, a primary focus in reducing the risk must be to keep nuclear material and nuclear weapons from being stolen by continually improving their security, as agreed at the Nuclear Security Summit in Washington in April 2010.

Surveillance Desirable: Terror Threat—Answers to “Nuclear Materials Unavailable”

1. Materials are available—North Korea, Pakistan, Russia

Samuel Kane, PREVENTING NUCLEAR TERRORISM: NUCLEAR SECURITY, THE NONPROLIFERATION REGIME, AND THE THREAT OF TERRORIST NUKES, Global Solutions, 2012, p. 8.

The threat of nuclear materials and technology falling into terrorist hands by such means is very real, and is one that this paper will seek to analyze. In particular, this paper will focus on three current members of the nuclear weapons club that represent the most likely sources for a terrorist-controlled nuclear weapon: Russia, Pakistan, and North Korea. Due to a range of factors, ranging from insecure facilities to radicalized personnel, these three states stand out as the most prominent threats to serve as facilitators, intentional or not, for an act of nuclear terrorism. However, while the prospect of nuclear assets from these three countries falling into terrorist hands is a serious threat, it is one that can be overcome through a combination of efforts by the states themselves, the United States, and the broader international community.

2. Plenty of poorly-secured research reactors have enough fissile material to make a bomb

Matthew Bunn, Associate professor, Public Policy, Harvard University, Testimony before the Canadian Special Senate Committee on Anti-Terrorism, 6--11--12,

http://belfercenter.ksg.harvard.edu/publication/22127/special_senate_committee_on_antiterrorism.html?breadcrumb=%2Fexperiments%2F368%2Fmatthew_bunn, accessed 4-4-13.

At the over 100 research reactors in the world that still use highly enriched uranium for their fuel, the security measures in place are often extremely modest. Some of these materials -- but by no means all -- have enough material on site to make a nuclear bomb. As all of the cases of theft of highly enriched uranium or plutonium where we know how it happened were perpetrated by insiders. Therefore, protection against insiders is particularly important and in many countries still requires improvement.

3. Materials are available--Russian materials are not secure

Samuel Kane, PREVENTING NUCLEAR TERRORISM: NUCLEAR SECURITY, THE NONPROLIFERATION REGIME, AND THE THREAT OF TERRORIST NUKES, Global Solutions, 2012, p. 1.

In Russia, the threat lies primarily in the form of terrorist groups stealing nuclear materials from Russian facilities. The questionable security of Russian nuclear facilities has its roots in the immediate aftermath of the Cold War, when the Soviet collapse left Russia with the responsibility of securing the USSR's vast nuclear arsenal, a task for which the nascent Russian Federation was vastly underprepared for. Recognizing the threat that a porous Russian nuclear complex posed to the national security of the United States, the American government has, in the years since the end of the Cold War, partnered with Russia in a variety of nuclear security initiatives, in order to reduce the threat of nuclear theft from Russian facilities. However, while the security of the Russian arsenal is undoubtedly better than it was twenty years ago, much work remains to be done.

4. Russian nuclear security is weak despite current U.S. aid

Samuel Kane, PREVENTING NUCLEAR TERRORISM: NUCLEAR SECURITY, THE NONPROLIFERATION REGIME, AND THE THREAT OF TERRORIST NUKES, Global Solutions, 2012, p. 13-14.

Despite the success stories that CTR and “Megatons to Megawatts” represent, Russia's nuclear security remains a liability. In particular, while the Nunn-Lugar initiative has certainly been successful in reducing the size of Russia's nuclear arsenal, concerns exist that it has failed to sufficiently upgrade security within the country's nuclear infrastructure. The responsibility for ensuring that these upgrades are made lies with the US Department of Energy. Specifically, this task falls under the purview of the National Nuclear Security Administration (NNSA), which sends managers and technicians from the US to Russia in order to supervise local officials in their installation and implementation of security upgrades. As William Langewiesche pointed out in a 2006 article for The Atlantic, the NNSA's work itself is not the main factor contributing to the Russian nuclear complex's lingering security problems. Rather, this issue can be attributed to two other factors. First, the task of upgrading Russia's nuclear security apparatus is an immense one, as evidenced by Langewiesche's assertion, referenced in Section 1, that, “Over the years, the NNSA has identified approximately 220 buildings at fifty-two sites...that are in dire need of treatment.” Second, many NNSA officials have expressed doubts about the strength of the Russian commitment to nuclear security, and have argued that “as soon as US funding ends, [the improvements made by the NNSA] will slip into disrepair.” Of course, given the current fiscal concerns dominating American politics, the US government cannot be expected to continue pouring resources into the Russian nuclear complex indefinitely. In light of this reality, Russia's apparently- tenuous commitment to safeguarding its nuclear resources is troubling, to say the least.

Surveillance Desirable: Terror Threat—Answers to “Nuclear Threat Exaggerated”

1. Al Qaeda and some other groups are seeking nuclear weapons, would use them

Matthew Bunn, Associate Professor, Public Policy, Kennedy School of Government, Harvard University, SECURING THE BOMB 2010, 4—10, p. 13-14.

Most terrorist groups are focused on small-scale violence to attain local objectives. For them, the old adage that “terrorists want a lot of people watching, not a lot of people dead” holds true, and nuclear weapons are likely to be irrelevant or counterproductive for their goals. But a small set of terrorists with global ambitions and nihilistic visions clearly are eager to get and use a nuclear bomb. Osama bin Laden has called the acquisition of nuclear weapons or other weapons of mass destruction a “religious duty.” For years, al Qaeda operatives have repeatedly expressed the desire to inflict a “Hiroshima” on the United States. Al Qaeda operatives have made repeated attempts to buy nuclear material for a nuclear bomb, or to recruit nuclear expertise. Shortly before the 9/11 attacks, for example, bin Laden and Ayman al-Zawahiri met with two senior Pakistani nuclear scientists to discuss nuclear weapons. Former CIA Director George Tenet reports that the two provided al Qaeda with a rough sketch of a nuclear bomb design, and that U.S. officials were so concerned about the activities of the “charity” they had established (whose board of directors also included a range of senior retired military officers, and which reportedly also offered nuclear weapons help to Libya) that President Bush directed him to fly to Pakistan and discuss the matter directly with Pakistani President Pervez Musharraf. Sultan Bashiruddin Mahmud, the more senior of the two, had long argued that Pakistan’s nuclear weapons rightfully belonged to the whole worldwide “ummah,” or Muslim community, and had advocated sharing nuclear weapons technology.

2. Al Qaeda is seeking a bomb, and could build one if they obtain the material—would be able to smuggle it into the U.S.

Matthew Bunn, Associate Professor, Public Policy, Kennedy School of Government, Harvard University, SECURING THE BOMB 2010, April 2010, p. v.

Several facts frame the danger: • Al Qaeda is seeking nuclear weapons and has repeatedly attempted to acquire the materials and expertise needed to make them. • Numerous studies by the U.S. and other governments have concluded that it is plausible that a sophisticated terrorist group could make a crude nuclear bomb if it got enough of the needed nuclear materials. • There have been over 18 documented cases of theft or loss of plutonium or highly enriched uranium (HEU), the essential ingredients of nuclear weapons. Peace activists have broken into a Belgian base where U.S. nuclear weapons are reportedly stored; two teams of armed men attacked a site in South Africa where hundreds of kilograms of HEU are stored; and Russian officials have confirmed that terrorist teams have carried out reconnaissance at Russian nuclear weapon storage facilities. • The immense length of national borders, the huge scale of legitimate traffic, the myriad potential pathways across these borders, and the small size and weak radiation signal of the materials needed to make a nuclear bomb make nuclear smuggling extraordinarily difficult to stop.

Surveillance Desirable: Terror Threat—Answers to “Won’t Go Nuclear” (General)

1. Threat of nuclear terrorism is high--want to use the weapons

Matthew Bunn, Associate Professor, Public Policy, Harvard University, Colonel Yuri Morozov, Professor, Russian Academy of Military Sciences, Rolf Mowatt Larssen, Senior Fellow, Harvard University, Simon Saradzhyan, Fellow, Harvard University, William Tobey, Senior Fellow, Harvard University, Viktor I. Yesin, Senior Fellow, Russian Academy of Sciences, and Pavel S. Zolotarev, Deputy Director, U.S.A. and Canadian Institute, Russian Academy of Sciences, THE U.S.-RUSSIA JOINT THREAT ASSESSMENT ON NUCLEAR TERRORISM, 5--11, p. 12.

Terrorists are aspiring to plot and execute attacks of increasingly catastrophic proportions. Terrorist groups have actively sought to acquire nuclear weapons. The nuclear terrorist threat is far greater today than it was during the Cold War, as a result of the confluence of four trends in the post-Cold War era: the rise of unlimited terrorism, i.e. terrorist groups who believe their objectives will be served by inflicting maximum possible damage, unconstrained by inhibitions created by concern that massive attacks might undercut political objectives by inspiring revulsion; the aging nature of nuclear weapons technology, which is no longer at the leading edge of science, at least for simple but effective designs; the vulnerability of weapons-usable nuclear material to theft or diversion; and globalization, which has given terrorists increasing access to reliable information and access to materials, designs, and potential victims.

2. Groups are not self-deterred--want to commit mass violence

Matthew Bunn, Associate Professor, Public Policy, Harvard University, Colonel Yuri Morozov, Professor, Russian Academy of Military Sciences, Rolf Mowatt Larssen, Senior Fellow, Harvard University, Simon Saradzhyan, Fellow, Harvard University, William Tobey, Senior Fellow, Harvard University, Viktor I. Yesin, Senior Fellow, Russian Academy of Sciences, and Pavel S. Zolotarev, Deputy Director, U.S.A. and Canadian Institute, Russian Academy of Sciences, THE U.S.-RUSSIA JOINT THREAT ASSESSMENT ON NUCLEAR TERRORISM, 5--11, p. 42.

Terrorism is but one means of achieving the political goals of separatists and representatives of other political movements. Types of terrorism include ethnic terrorism, religious terrorism, extremist terrorism, economic terrorism, technological terrorism and state terrorism. Most terrorist groups are unlikely to be interested in causing mass violence on a nuclear scale, which might do more to undermine than to promote their political objectives. But as the cases of al-Qaeda, the North Caucasus groups, and Aum Shinrikyo demonstrate, some terrorists do seek to inflict mass casualties, and have sought nuclear weapons. With three groups having already gone down this road in the last 15 years, the world cannot expect that they will be the last. The long-term threat is broader than al-Qaeda associates and North Caucasus groups, is not confined to Islamic extremists, and is likely here to stay. Some aspects of contemporary terrorism differ greatly from the terrorism of the 19th and 20th centuries. Modern terrorism has the following distinct features: • It poses a much greater threat to public safety, with some terrorist groups seeking to maximize casualties and damage, without restraint or concern that backlash could threaten their political objectives. • It is public in nature, in that its attacks are designed to provoke a specific public reaction to the terrorist's narrative, as well as a specific government response. • Its main goal is to create an atmosphere of fear to coerce the entire society. • It is characterized by acts of violence inflicted upon one group of people with the aim of influencing a different group of people.

Surveillance Desirable: Terror Threat—Answers to “Won’t Go Nuclear” (Al Qaeda)

1. Al Qaeda's evolving decentralization exacerbates the threat--securing materials is vital to stopping nuclear terrorism

Sarah Williams, fellow, Center for Science, Technology, and Security Policy at the American Association for the Advancement of Science and coordinator, Fissile Materials Working Group, "After bin Laden: Nuclear Terrorism Still a Top Threat," BULLETIN OF THE ATOMIC SCIENTISTS, 5--13--11, <http://www.thebulletin.org/web-edition/columnists/fissile-materials-working-group/after-bin-laden-nuclear-terrorism-still-top-t>, accessed 4-4-13.

While Al Qaeda's anti-American ideology is unlikely to change after bin Laden's death, the loss of the group's founder and figurehead could affect Al Qaeda's structure. According to the Atlantic Council's J. Peter Pham, regional "branches" and "franchises" of the terrorist organization gained power during the decade that bin Laden was in hiding, and while united by their loyalty to Al Qaeda's mission, they are not necessarily subject to orders from a central leadership. The growing influence, strength, and operational capacity of these regional organizations (Al Qaeda in the Arabian Peninsula and Al Qaeda in the Islamic Maghreb, for example) are of particular concern with respect to the threat of nuclear terrorism. The best way to prevent Al Qaeda subgroups -- ideologically aligned, geographically disparate, and operating under regional leadership -- from gaining access to nuclear material is to secure existing sites and eliminate superfluous storage sites. Enough nuclear material to make tens of thousands of nuclear devices exists in dozens of locations worldwide. Without being able to predict how bin Laden's death might alter the operational capacity of Al Qaeda, a US priority must be securing this potential source material.

2. Al Qaeda and other terrorist groups are still committed to nuclear acquisition and use

James F. Smith, Harvard Kennedy School Communications, "The Threat of Nuclear Terror," HARVARD GAZETTE, 6--6--11, <http://news.harvard.edu/gazette/story/2011/06/the-threat-of-nuclear-terror/>, accessed 4-4-13.

"The joint threat assessment accomplishes something that so far governments have been unable to do: gauge the threat of nuclear terrorism from differing national perspectives, and thereby form the basis for effective action to defeat it," said Tobey. "This will help to overcome the No. 1 barrier to improved nuclear security — complacency." The assessment examines potential terrorist pathways to a nuclear attack, among them buying or stealing an existing weapon, or getting highly enriched uranium or plutonium and fashioning a crude nuclear bomb of their own, which the study warns is distressingly plausible. It also concludes that while the killing of al Qaeda leader Osama bin Laden damages the groups' capacity to carry out nuclear terrorism, surviving leaders retain nuclear terror ambitions. The joint report documents that al Qaeda has been working for years to acquire the materials and expertise needed to make a crude nuclear bomb, getting as far as carrying out explosive tests for their nuclear program in the Afghan desert. The report outlines the steps that terrorists could follow and envisions how such a terrorist plot might be structured — and how countries should work together to stop it. The study notes that, in addition to al Qaeda, terrorists from the North Caucasus region remain committed to carrying out catastrophic attacks, have carried out reconnaissance at nuclear weapons storage sites, have plotted to hijack a submarine with nuclear weapons on board, have planted radiological materials in Moscow, and have repeatedly threatened to attack nuclear power plants. These groups include factions in Chechnya, Dagestan, Ingushetia, and elsewhere.

3. Al Qaeda remains committed to obtaining and using a nuclear bomb

Matthew Bunn, Associate Professor, Public Policy, Harvard University, Colonel Yuri Morozov, Professor, Russian Academy of Military Sciences, Rolf Mowatt Larssen, Senior Fellow, Harvard University, Simon Saradzhyan, Fellow, Harvard University, William Tobey, Senior Fellow, Harvard University, Viktor I. Yesin, Senior Fellow, Russian Academy of Sciences, and Pavel S. Zolotarev, Deputy Director, U.S.A. and Canadian Institute, Russian Academy of Sciences, THE U.S.-RUSSIA JOINT THREAT ASSESSMENT ON NUCLEAR TERRORISM, 5--11, p. 10-11.

Al-Qaeda has sought nuclear weapons for almost two decades. The group has repeatedly attempted to purchase stolen nuclear material or nuclear weapons, and has repeatedly attempted to recruit nuclear expertise. Al-Qaeda reportedly conducted tests of conventional explosives for its nuclear program in the desert in Afghanistan. The group's nuclear ambitions continued after its dispersal following the fall of the Taliban regime in Afghanistan. Recent writings from top al-Qaeda leadership are focused on justifying the mass slaughter of civilians, including the use of weapons of mass destruction, and are in all likelihood intended to provide a formal religious justification for nuclear use. While there are significant gaps in coverage of the group's activities, al-Qaeda appears to have been frustrated thus far in acquiring a nuclear capability; it is unclear whether the group has acquired weapons-usable nuclear material or the expertise needed to make such material into a bomb. Furthermore, pressure from a broad range of counter-terrorist actions probably has reduced the group's ability to manage large, complex projects, but has not eliminated the danger. However, there is no sign the group has abandoned its nuclear ambitions. On the contrary, leadership statements as recently as 2008 indicate that the intention to acquire and use nuclear weapons is as strong as ever.

Surveillance Desirable: Terror Threat—Answers to “Won’t Go Nuclear” (Al Qaeda)

[cont’d]

4. Al Qaeda wants to use nuclear weapons

Matthew Bunn, Associate Professor, Public Policy, Harvard University, Colonel Yuri Morozov, Professor, Russian Academy of Military Sciences, Rolf Mowatt Larssen, Senior Fellow, Harvard University, Simon Saradzhyan, Fellow, Harvard University, William Tobey, Senior Fellow, Harvard University, Viktor I. Yesin, Senior Fellow, Russian Academy of Sciences, and Pavel S. Zolotarev, Deputy Director, U.S.A. and Canadian Institute, Russian Academy of Sciences, THE U.S.-RUSSIA JOINT THREAT ASSESSMENT ON NUCLEAR TERRORISM, 5--11, p. 23-24.

Obtaining high-end weapons of mass destruction has been a high priority for a terrorist group that harbors ambitions of defeating the U.S. and its allies, overthrowing so-called apostate regimes, restoring the Islamic Caliphate, and expanding it to cover the globe. Al-Qaeda leaders have consistently noted in public pronouncements spanning more than two decades that they are willing to employ all available means at their disposal to achieve their objectives. They have mastered the art of surprise with each successive attack. In this context, they do not appear to be interested in chemical, biological, or radiological/nuclear weapons for their own sake, apart from their potential effectiveness against specific targets. The leadership’s pursuit of a nuclear bomb in parallel to the group’s known efforts to develop anthrax in the late 1990’s suggests that either a nuclear or a biological weapon would be suitable for use in a future attack that was being contemplated, depending on which means (if any) they could acquire. Recent writings from top al-Qaeda leadership (2003 and 2008) offer a meticulously researched religious ruling, or fatwa, for the use of weapons of mass destruction in the mass slaughter of civilians. It is clear that the group desires high-end WMD, whether in the form of biological weapons or of nuclear weapons capable of killing millions of people and causing mass economic damage. The al-Qaeda leadership’s justification for the use of WMD on religious grounds cannot be dismissed as a theological exercise. In all probability, the group’s leaders are explaining why the use of WMD is necessary because they are actively planning to use these weapons; if 9/11 was a declaration of war against America, a Hiroshima bomb is a way to win the war. Nuclear and “big bio” weapons are desirable because they can produce global economic disruption, cause mass casualties, and perhaps most importantly, create widespread doubts concerning world order and governance. In this context, there are chilling similarities between the warning and planning cycle associated with the 9/11 attack, and rituals associated with al-Qaeda’s WMD statements. Osama bin Laden issued 1998 fatwa that served as a harbinger of the 9/11 attack that followed three years later. The al-Qaeda leader’s declaration of war against America not only fulfilled a religious obligation, it launched a secret planning process for an unprecedented attack that was carried out with devastating effect. The timing of al-Qaeda deputy leader Ayman al-Zawahiri’s 2008 fatwa—which meticulously justifies an unprecedented attack on an almost unimaginable scale of destruction—may have started the clock ticking for an attack capable of fulfilling al-Zawahiri’s promise to elevate the level of violence to a new scale. The high-end scale of al-Qaeda’s intent to produce mass destruction is clearly evident from a 26- page fatwa entitled A Treatise on the Legal Status of Using Weapons of Mass Destruction Against Infidels, published by radical Saudi cleric Nasir al-Fahd on May 21, 2003. Al-Fahd offered three central arguments justifying the use of WMD. First, one kills in a good manner only when one can. If those engaged in jihad cannot do so, for example when they are forced to bomb, destroy, burn or flood, it is permissible. Second, one avoids killing women and children only when one can distinguish them from men. If one cannot do so, as when infidels make a night attack or invade, a Muslim may be killed as collateral damage in killing the fighters. And third, killing a Muslim is forbidden and not permitted; but if those engaged in jihad are forced to kill him because they cannot repel the infidels or fight them otherwise, it is permitted, as when the Muslim is being used as a living shield. But al-Fahd also argued that using nuclear weapons against U.S. civilians was justified because it was a proportionate response to the harms inflicted on the Islamic community: “If a bomb that killed 10 million of them and burned as much of their land as they have burned Muslims’ land were dropped on them, it would be permissible.”

Surveillance Desirable: Answers to “Chilling Effect”**- There is no chilling effect—the empirical records shows this to be the case**

Eric Posner, Professor, Law, University of Chicago, “Secrecy and Freedom,” NEW YORK TIMES, Room for Debate, 6—9—13, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined>, accessed 10-4-13. This brings me to another valuable point you made, which is that when people believe that the government exercises surveillance, they become reluctant to exercise democratic freedoms. This is a textbook objection to surveillance, I agree, but it also is another objection that I would place under “theoretical” rather than real. Is there any evidence that over the last 12 years, during the flowering of the so-called surveillance state, Americans have become less politically active? More worried about government suppression of dissent? Less willing to listen to opposing voices? All the evidence points in the opposite direction. Views from the extreme ends of the political spectrum are far more accessible today than they were in the past. It is infinitely easier to get the Al Qaeda perspective today — one just does a Google search — than it was to learn the Soviet perspective 40 years ago, which would have required one to travel to one of the very small number of communist bookstores around the country. It is hard to think of another period so full of robust political debate since the late 1960s — another era of government surveillance.

Surveillance Desirable: Answers to “Illegal / Overreach”

1. The NSA program is not lawless—it has been vetted by all three branches

Stewart Baker, former Assistant Secretary for Policy, Department of Homeland Security, “Why the NSA Needs Your Phone Calls,” FOREIGN POLICY, 6—6—13, www.foreignpolicy.com/articles/2013/06/06/why_the_nsa_needs_your_phone_calls, accessed 10-12-13.

In fact, it's a near certainty that the legal theory behind orders of this sort has been carefully examined by all three branches of the government and by both political parties. As the Guardian story makes clear, Sen. Ron Wyden has been agitating for years about what he calls an interpretation of national security law that seems to go beyond anything the American people understand or would support. He could easily have been talking about orders like this. So it's highly likely that the law behind this order was carefully vetted by both intelligence committees, Democrat-led in the Senate and Republican-led in the House. (Indeed, today the leaders of both committees gave interviews defending the order.) And in the executive branch, any legal interpretations adopted by George W. Bush's administration would have been carefully scrubbed by President Barack Obama's Justice Department.

2. The Authorization of Use of Military Force (AUMF) makes NSA surveillance programs legal

John Yoo, Professor, Law, University of California, Berkeley, “The Terrorist Surveillance Program and the Constitution,” GEORGE MASON LAW REVIEW v. 14, 2007, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=975333, accessed 10-2-13.

Critics have argued that the NSA's electronic surveillance is illegal because the AUMF didn't explicitly mention wiretapping or surveillance. Of course it doesn't mention detentions, either, which the Supreme Court later upheld as authorized by Congress, in spite of a law on the books known as the Anti-Detention Act. Critics essentially argue that Congress must enact a grocery list of specific powers and otherwise the President cannot fight a war. For instance, FISA prohibits electronic surveillance within the United States without congressional permission. However, in the AUMF, Congress authorized the President “to use all necessary and appropriate force . . . [against those] he determines” were involved with the 9/11 attacks, or those who aid, support, or harbor those involved. Individuals who are communicating with suspected al Qaeda operatives after 9/11 are likely to fall within the scope of the AUMF. The power to use force impliedly includes the power to use surveillance and intelligence to find the targets. According to the critics, Congress authorized the President to pull the trigger, but also ordered him to wear a blindfold.

3. NSA activities are not illegal—they do not review content, any such activity is targeted at non-citizens

Michael Barone, American Enterprise Institute, “NSA Surveillance, if Ungentlemanly, Is not Illegal,” WASHINGTON EXAMINER, 6—11—13, <http://aei.org/article/foreign-and-defense-policy/defense/intelligence/nsa-surveillance-if-ungentlemanly-is-not-illegal/>, accessed 10-4-13.

Is the NSA surveillance of telephone records illegal? No, it has been authorized by the FISA Court under the FISA Act provisions passed by (a Democratic) Congress in 2008. The NSA is not entitled to listen to the contents of specific phone calls. It has to go back to the FISA Court for permission to do that. Under the Supreme Court's 1979 *Smith v. Maryland* decision, the government can collect evidence of phone numbers called, just as the government can read the addresses on the outside of an envelope. Snowden presented no evidence that the NSA is abusing its powers by accessing the private information of those with obnoxious opinions. There is, so far anyway, no evidence of the kind of political targeting committed by the Internal Revenue Service. Instead, the NSA is looking for patterns of unusual behavior that might indicate calls to and from terrorists. This data mining relies on the use of algorithms sifting through Big Data, much like the data mining of Google and the Obama campaign. Snowden also exposed the NSA's Prism program, which does surveil the contents of messages -- but only those of suspected terrorists in foreign countries. During George W. Bush's administration, many journalists and Democrats assailed this as “domestic wiretapping.” But the only time people here are surveilled is when they are in contact with terrorism suspects in foreign countries. The right of the government to invade people's privacy outside the United States is, or should not be, in question.

Surveillance Desirable: Answers to “Illegal / Overreach” [cont’d]

4. Obsolete laws should not stop us from acting to foil terrorist attacks

John Yoo, visiting scholar, American Enterprise Institute, “Why We Endorsed Warrantless Wiretaps,” WALL STREET JOURNAL, 7—16—09, <http://aei.org/article/foreign-and-defense-policy/defense/why-we-endorsed-warrantless-wiretaps/>, accessed 10-3-13.

It is absurd to think that a law like FISA should restrict live military operations against potential attacks on the United States. Congress enacted FISA during the waning days of the Cold War. As the 9/11 Commission found, FISA's wall between domestic law enforcement and foreign intelligence proved dysfunctional and contributed to our government's failure to prevent the 9/11 attacks. Under FISA, to obtain a judicial wiretapping warrant the government is supposed to show probable cause that a specified target is a foreign agent. Unlike, say, Soviet spies working under diplomatic cover, terrorists are hard to identify. Yet they are vastly more dangerous. Monitoring their likely communications channels is the best way to track and stop them. Building evidence to prove past crimes, as in the civilian criminal system, is entirely beside the point. The best way to find an al Qaeda operative is to look at all email, text and phone traffic between Afghanistan and Pakistan and the U.S. This might involve the filtering of innocent traffic, just as roadblocks and airport screenings do. In FISA, President Bush and his advisers faced an obsolete law not written with live war with an international terrorist organization in mind. It was to meet such emergency circumstances that the Founders designed the presidency. As John Locke first observed, foreign threats "are much less capable to be directed by antecedent, standing, positive laws." Legislatures are too slow and their members too numerous to respond effectively to unforeseen situations. Only the executive can act to protect the "security and interest of the public." The power to protect the nation, said Alexander Hamilton in the Federalist, "ought to exist without limitation," because "it is impossible to foresee or define the extent and variety of national exigencies, or the correspondent extent & variety of the means which may be necessary to satisfy them." To limit the president's constitutional power to protect the nation from foreign threats is simply foolhardy. Hamilton observed that "decision, activity, secrecy, and dispatch will generally characterize the proceedings of one man, in a much more eminent degree, than the proceedings of any greater number." "Energy in the executive," he reiterated, "is essential to the protection of the community against foreign attacks."

5. FISA regulations are too slow and cumbersome to deal with some terror threats

John Yoo, Professor, Law, University of California, Berkeley, “The Terrorist Surveillance Program and the Constitution,” GEORGE MASON LAW REVIEW v. 14, 2007, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=975333, accessed 10-2-13.

In this world of rapidly shifting e-mail addresses, multiple cell phone numbers, and internet communications, FISA imposes slow and cumbersome procedures on our intelligence and law enforcement officers. These laborious checks are based on the assumption that we still remain within the criminal justice system, and are looking backward in order to conduct prosecutions of those who have perpetrated crimes or infiltrated the government, rather than operating within the national security system, which looks forward in order to prevent deadly surprise attacks on the American people. FISA requires a lengthy review process, in which special FBI and DOJ lawyers prepare an extensive package of facts and law to present to the Federal Intelligence Surveillance Court (“FISC”). The Attorney General must personally sign the application, and another high-ranking national security officer, such as the President’s National Security Advisor or the Director of the FBI, must certify that the information sought is for foreign intelligence. It takes time and a great deal of work to prepare the warrant applications, which can run 100 pages long. While there is an emergency procedure that allows the Attorney General to approve a wiretap for 72 hours without a court order, it can only be used if there is no time to obtain an order from the FISC, and the Attorney General determines that the wiretap satisfies FISA’s other requirements. Thus, the Attorney General could not use the emergency procedure if the probable cause standard was not met.

Surveillance Desirable: Answers to “Privacy”—Citizen Surveillance

1. Current minimization practices protect citizen privacy

Stewart Baker, former Assistant Secretary for Policy, Department of Homeland Security, “Why the NSA Needs Your Phone Calls,” FOREIGN POLICY, 6—6—13, www.foreignpolicy.com/articles/2013/06/06/why_the_nsa_needs_your_phone_calls, accessed 10-12-13.

The technique that squares that circle is minimization. As long as the minimization rules require that all searches of the collected data must be justified in advance by probable cause, Americans are protected from arbitrary searches. In the standard law enforcement model that we're all familiar with, privacy is protected because the government doesn't get access to the information until it presents evidence to the court sufficient to identify the suspects. In the alternative model, the government gets possession of the data but is prohibited by the court and the minimization rules from searching it until it has enough evidence to identify terror suspects based on their patterns of behavior. That's a real difference. Plenty of people will say that they don't trust the government with such a large amount of data -- that there's too much risk that it will break the rules -- even rules enforced by a two-party, three-branch system of checks and balances. When I first read the order, even I had a moment of chagrin and disbelief at its sweep. But for those who don't like the alternative model, the real question is "compared to what"? Those who want to push the government back into the standard law enforcement approach of identifying terrorists only by name and not by conduct will have to explain how it will allow us to catch terrorists who use halfway decent tradecraft -- or why sticking with that model is so fundamentally important that we should do so even if it means more acts of terrorism at home.

2. The NSA program actively tries to limit the information that it collects about Americans

Stewart Baker, former Assistant Secretary for Policy, Department of Homeland Security, “Why the NSA Needs Your Phone Calls,” FOREIGN POLICY, 6—6—13, www.foreignpolicy.com/articles/2013/06/06/why_the_nsa_needs_your_phone_calls, accessed 10-12-13.

Ah, you say, but the scandal here isn't what has been done illegally -- it's what has been done legally. Even if it's lawful, how can the government justify spying on every American's phone calls? It can't. No one has repealed the laws that prohibit the National Security Agency (NSA) from targeting Americans unless it has probable cause to believe that they are spies or terrorists. So under the law, the NSA remains prohibited from collecting information on Americans. On top of that, national security law also requires that the government "minimize" its collection and use of information about Americans -- a requirement that has spawned elaborate rules that strictly limit what the agency can do with information it has already collected. Thus, one effect of "post-collection minimization" is that the NSA may find itself prohibited from looking at or using data that it has lawfully collected. I would not be surprised to discover that minimization is the key to this peculiarly two-party, three-branch "scandal." That is, while the order calls for the collection of an enormous amount of data, much of it probably cannot actually be searched or used except under heavy restrictions. (If I'm right, the administration is likely to find itself forced quite quickly to start talking about minimization, perhaps in considerable detail.)

Surveillance Desirable: Answers to “Privacy”—Dead

1. We need to embrace an updated notions of privacy—it is not secrecy, but a lack of scrutiny of our activities that can be observed

Paul Rosenzweig, visiting fellow, Heritage Foundation, Testimony before the Senate Subcommittee on Oversight of Government Management, the Federal Workforce and the District of Columbia Committee on Homeland Security and Governmental Affairs, 7—31—12, <http://www.heritage.org/research/testimony/2012/08/the-state-of-privacy-and-security-our-antique-privacy-rules>, accessed 10-3-13.

Privacy is really a misnomer. What it reflects is a desire for independence of personal activity, a form of autonomy. We protect that privacy in many ways. Sometimes we do so through secrecy which effectively obscures both observation of conduct and the identity of those engaging in the conduct. In other instances we protect the autonomy directly. Even though conduct is observed and the actor identified, we provide direct rules to limit action as, for example, in the criminal context where we have an exclusionary rule to limit the use of illegally collected evidence. The concept of privacy that most applies to the new information technology regime is the idea of anonymity or “practical obscurity,” a middle ground where observation is permitted that is, we expose our actions in public but we are not subject to identification or scrutiny. The information data-space is suffused with information of this middle-ground sort, e.g., bank account transactions, phone records, airplane reservations, and Smartcard travel logs to name but a few. They constitute the core of transactions and electronic signature or verification information available in cyberspace. The anonymity that one has in respect of these transactions is not terribly different from “real-world anonymity.” Consider, as an example, the act of driving a car. It is done in public, but one is generally not subject to routine identification and scrutiny. Protecting the anonymity we value requires, in the first instance, defining it accurately. One might posit that anonymity is, in effect, the ability to walk through the world unexamined. That is, however, not strictly accurate, for our conduct is examined numerous times every day. Sometimes the examination is by a private individual for example, one may notice that the individual sitting next to them on the train is wearing a wedding ring. Other routine examinations are by governmental authorities—the policeman in the car who watches the street or the security camera at the bank or airport, for example. As we drive down the road, any number of people might observe us.

2. Our privacy laws are antiquated and we should have no expectation of online anonymity

Paul Rosenzweig, visiting fellow, Heritage Foundation, Testimony before the Senate Subcommittee on Oversight of Government Management, the Federal Workforce and the District of Columbia Committee on Homeland Security and Governmental Affairs, 7—31—12, <http://www.heritage.org/research/testimony/2012/08/the-state-of-privacy-and-security-our-antique-privacy-rules>, accessed 10-3-13.

Cyber dataveillance is here to stay whether we like it or not. The only question is when and how we monitor and control the government’s use of the techniques so that we get the benefits of the growth in data surveillance without the potential harms to civil liberties. As should be evident, the use of such analytical tools is not without risks. The same systems that sift layers of data to identify concealed terrorist links are just as capable, if set to the task, of stripping anonymity from many other forms of conduct—personal purchases, politics, and peccadilloes. The question then becomes how do we empower data analysis for good purposes while providing oversight mechanisms for deterring malfeasant uses? Our current privacy-protective architecture, or, if one prefers, our anonymity-protective architecture, is simply not up to the task. It is, to a very real degree, an antique relic of the last century. The relevant Supreme Court precedents date from the 1970s, as does the 1974 Privacy Act. Is it any wonder that the current structure of law does not match the technological reality? The “third party doctrine” developed by the Supreme Court in two 1970-era cases—*United States v. Miller* and *Smith v. Maryland*—at the dawn of the computer era, means that information you disclose to a third party is not protected by the Fourth Amendment. In the context of data privacy, that means that there is no constitutional protection against the collection and aggregation of your cyber data (credit card purchase and the like) for purposes of data analysis and piercing the veil of anonymity.

Surveillance Desirable: Answers to “Privacy”—Dead [cont’d]

3. Online privacy is dead—private data collection

Paul Rosenzweig, visiting fellow, Heritage Foundation, Testimony before the Senate Subcommittee on Oversight of Government Management, the Federal Workforce and the District of Columbia Committee on Homeland Security and Governmental Affairs, 7—31—12, <http://www.heritage.org/research/testimony/2012/08/the-state-of-privacy-and-security-our-antique-privacy-rules>, accessed 10-3-13.

Ten years ago, surveying the technology of the time which, by and large, was one hundred times less powerful than today’s data processing capacity Scott McNealy, then-CEO of Sun Microsystems, said, “Privacy is dead. Get over it.” He was, it seems, slightly wrong. Pure privacy—that is, the privacy of activities in your own home—remains reasonably well-protected. What has been lost, and will become even more so increasingly, is the anonymity of being able to act in public (whether physically or in cyberspace) without anyone having the technological capacity to permanently record and retain data about your activity for later analysis. Today, large data collection and aggregation companies, such as Experian and Axicom, may hire retirees to harvest, by hand, public records from government databases. Paper records are digitized and electronic records are downloaded. These data aggregation companies typically hold birth records, credit and conviction records, real estate transactions and liens, bridal registries, and even kennel club records. One company, Acxiom, estimates that it holds on average approximately 1,500 pieces of data on each adult American. Since most, though not all, of these records are governmental in origin, the government has equivalent access to the data, and what they cannot create themselves they can likely buy or demand from the private sector. The day is now here when anyone with enough data and sufficient computing power can develop a detailed picture of any identifiable individual. That picture might tell your food preferences or your underwear size. It might tell something about your terrorist activity. Or your politics.

Surveillance Desirable: Answers to “Privacy”—Fourth Amendment

1. Strict adherence to the Fourth Amendment would make it impossible to defeat the terrorist threat

John Yoo, Professor, Law, University of California-Berkeley, “The NSA’s Surveillance: No Clear Constitutional Violations,” NATIONAL REVIEW, The Corner, 6—7—13, www.nationalreview.com/corner/350498/nsas-surveillance-no-clear-constitutional-violations-john-yoo, accessed 10-2-13.

The revelation of broad e-mail surveillance is more troubling, but it is because we don’t know the program’s scope. If the program only intercepts the content of e-mails for foreigners abroad, as is being reported, there is no constitutional violation. As the Supreme Court has made clear, the Fourth Amendment does not protect the communications of non-U.S. persons that take place abroad. In fact, the Justices reached that conclusion because they observed that it would be impossible for the U.S. to fight a war against a foreign enemy if limited by the Fourth Amendment. Allowing the government to intercept foreign, potentially enemy signals intelligence abroad without a warrant recognizes the reality of war, as opposed to the precise targeting of communications that would apply if domestic law enforcement were the framework.

2. The metadata program does not run afoul of the Fourth Amendment—you have no privacy for the numbers dialed, just the content of the communications

John Yoo, Professor, Law, University of California-Berkeley, “The NSA’s Surveillance: No Clear Constitutional Violations,” NATIONAL REVIEW, The Corner, 6—7—13, www.nationalreview.com/corner/350498/nsas-surveillance-no-clear-constitutional-violations-john-yoo, accessed 10-2-13.

The latest Obama administration controversy will not prove as bad as it first seems. Apparently, the administration has been asking Verizon for all of the “metadata” on all of its customers’ calling — the phone numbers called and received, but not the content of the calls themselves. In the days after the September 11, 2001 attacks, the Bush administration’s Justice Department (in which I served) approved a program that may have relied on similar technology, but was far narrower in scope. Both programs, however, seek to use communications coming into the United States from a known terrorist abroad to identify an al-Qaeda network within the country. The program does not represent a violation of the Constitution because the Fourth Amendment does not protect dialed phone numbers, in contrast to the content of the communications, because individuals lose privacy over those numbers when they are given to the phone company. The Constitution protects the content of the communications, whether it be a phone call, e-mail, or old-fashioned letter. And Congress approved a change to the FISA statute to allow such collection, and a court of federal judges approved it. And as commander-in-chief, the president has the wartime authority to find and intercept enemy communications, known as signals intelligence. Analyzing such metadata — what is sometimes called data mining — is perhaps the most effective way to find terrorist cells in the U.S. and stop future attacks because the Obama administration has dropped our best methods for producing intelligence (the detention and interrogation of al-Qaeda leaders).

3. The metadata program is legal under the Fourth Amendment—multiple reasons

Steven G. Bradbury, Dechert, LLP, Testimony before the House Judiciary Committee, 7—17—13, <http://judiciary.house.gov/hearings/113th/07172013/Bradbury%2007172013.pdf>, accessed 10-2-13.

In terms of the background constitutional principles, it’s important to remember that the Fourth Amendment itself would not require a search warrant or other individualized court order for such data acquisition. A government request for a company’s business records is not a “search” within the meaning of the Fourth Amendment. Government agencies have authority under many federal statutes to issue administrative subpoenas without court approval for documents that are “relevant” to an authorized inquiry. In addition, grand juries have broad authority to subpoena records potentially relevant to whether a crime has occurred, and grand jury subpoenas also don’t require court approval. In the modern world of electronic storage and data compilation, reliance on the same “relevance” standard in these other contexts can also result in extremely expansive requests for business records. In addition, the Fourth Amendment does not require a warrant when the government seeks purely transactional information, or metadata, as distinct from the content of communications. This information is voluntarily made available to the phone company to complete the call and for billing purposes, and courts have therefore said there’s no reasonable expectation that it’s private. See *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979); *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 904-05 (9th Cir. 2008). I would stress, however, that section 215 is more restrictive than the Constitution demands, because it requires the approval of a federal judge. In this way, Congress in the PATRIOT Act adopted a requirement for judicial review and approval of FISA business records orders that is more protective of privacy and civil liberties interests than the Constitution would otherwise demand. And while the 215 order for metadata is extraordinary in terms of the amount of data acquired, it’s also extraordinarily narrow and focused in terms of the strict limitations placed on accessing the data at the back end.

Surveillance Desirable: Answers to “Privacy”—Fourth Amendment [cont’d]**4. Collecting metadata is clearly constitutional**

Paul Rosenzweig, visiting fellow, Heritage Foundation, “The NSA’s Phone Collection Order—It May Be Legal, but Is it Wise?” FOX NEWS, 6—7—13, www.heritage.org/research/commentary/2013/6/the-nsas-phone-collection-order-it-may-be-legal-but-is-it-wise, accessed 10-3-13.

In short, the order appears to give NSA blanket access to the records of Verizon customers' phone calls—foreign and domestic—made between April 25, when the order was signed, and July 19, when it expires. Of course, if the order is only the latest in a series of orders (as also seems likely), then the access may go back for quite some time. To a large degree this revelation it is not unexpected. We are a country still at war against Al Qaeda and its affiliates. As such, we need to have counterterrorism tools, such as Section 215 of the PATRIOT Act, which was apparently used in this case. And, though we don't yet know the details, it is important to note that since 9/11, the powerful tools have been modified and amended to maximize the protection of civil liberties to the extent possible. Here, the FISA court issued an order allowing for telephone calling data only, not the content of any calls. Such data are critical for link analysis -- connecting the dots between phone numbers in terrorist investigations. That is constitutional. Meta-data are not currently protected under the Fourth Amendment, and the large-scale collection of that meta-data remains lawful.

Surveillance Desirable: Answers to “Privacy”—General

1. No actual abuse is occurring—their claims are all hypotheticals

Bill Scher, Campaign for America’s Future, “The Liberal Case for High-Tech NSA Surveillance,” THE WEEK, 6—13—13, <http://theweek.com/article/index/245464/the-liberal-case-for-high-tech-nsa-surveillance>, accessed 10-13-13.

There is, in fact, a strong liberal case to make for America’s current use of surveillance to combat terrorism. Liberals are not libertarians or anarchists. Liberals believe in a proper use of government to maximize the common good, including public safety. What liberals have long opposed are abuses of power that harm individuals yet do nothing to keep us safe: systematic torture, racial profiling, FBI infiltration and disruption of civil rights groups, communist witch hunts, Japanese internment camps, the Palmer raids — the list goes on. Similarly, liberals oppose the abuse of political power to intimidate political opponents, such as the Bush administration’s purge of U.S. attorneys who wouldn’t pursue trumped up allegations of voter fraud, or Richard Nixon’s (thwarted) attempt to use the IRS to punish adversaries. In this case, such abuses did not occur. Glenn Greenwald, the civil libertarian activist/journalist who helped publish the leaked information in the Guardian, argued on MSNBC Monday that “the U.S. government is collecting under the aegis of the secret FISA court the telephone records of every single American on American soil, every single phone call they make, international, and local, and storing those telephone numbers in a database and constructing massive data files that enable all kinds of intrusive surveillance” (emphasis added). Not even Greenwald can claim that the government is actually practicing intrusive surveillance today. His argument is that intelligence officials might someday. The NSA has been engaged in this sort of surveillance ever since 9/11, under two presidents of decidedly different ideological outlooks, and two administrations with vastly different records on the use of political power. Yet not even the most strident civil libertarian has evidence that this “metadata” has been abused. Maybe someday some abominable security official or political hack will break the law and violate the Constitution with such abuse. But that’s a maybe that can be handled under our current laws and judicial system, should it ever occur.

2. NSA activities are directly targeted at stopping terrorism—they are not surveilling our everyday online activities

Froma Harrop, “Unjustified Hysteria Over the NSA Surveillance Program,” SEATTLE TIMES, 8—5—13, http://seattletimes.com/html/opinion/2021545910_harropcolumnnsahysteriaxml.html, accessed 10-3-13.

So hard as I try, I can’t fathom the manic outrage over the idea of a government computer raking through the metadata on Americans’ phone calls and emails. Metadata is about email addresses, numbers called and length of conversation. The computers don’t look at content — what I say or what is said to me. Where’s the big loss in privacy? For eons, law enforcement has been able to tap the phone records of suspects. You know the line in “Law & Order”: “Get me his luds (local usage details).” John Schindler is an expert on intelligence and terrorism at the U.S. Naval War College. He spent a decade with the NSA. Do I understand the basics? I ask him. Pretty much. First off, the front end, the collection of metadata, is all automated. The computer flags suspicious activity, but a human can’t look further without a FISA (Foreign Intelligence Surveillance Act) warrant. FISA warrants are granted for only two reasons: 1. Foreign espionage. 2. Foreign terrorism. If that human finds that someone has been emailing a known terrorist to discuss fine points of religion, that person still wouldn’t be a legitimate intelligence target, Schindler says. The conversation has to be about plotting terrorism. Agencies investigating drug trafficking, cyberattacks and other criminal activity have long complained about being denied access to NSA intelligence data. That’s because their searches are not directly connected to terrorism or foreign spying. Is this how it always works? “The media want to have a simple NSA,” Schindler responded, but intelligence operations can be complex and tricky. Information might be passed to the FBI, CIA or foreign security services. This can be a multination operation. So the answer is no, not always. “But the idea of 10,000 NSA agents looking at our pictures of cats and pornography is pure fantasy,” he remarked.

Surveillance Desirable: Answers to “Privacy”—General [cont’d]

3. Privacy concerns are ill-founded—we already give the government enormous quantities of information

Eric Posner, Professor, Law, University of Chicago, “Secrecy and Freedom,” NEW YORK TIMES, Room for Debate, 6—9—13, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined>, accessed 10-4-13. Jameel, I don’t see the need for systemic reform, nor do I see an offense to the Constitution. Indeed, I don’t even understand the nature of the objection to the National Security Agency programs. Exactly what harm did they cause? Two possibilities emerge from the current public discussion. 1. A general sense of creepiness that government officials know when we make phone calls, and for how long, or may even be reading our e-mail messages. Government should not look over our shoulders as we conduct our lives. 2. A fear that the government uses this information to undermine democracy — to blackmail, harass or embarrass critics, for example. The first objection strikes me as weak. We already give the government an enormous amount of information about our lives, and seem to have gotten used to the idea that an Internal Revenue Service knows our finances, or that an employee of a government hospital knows our medical history, or that social workers (if we are on welfare) know our relationships with family members, or that public school teachers know about our children’s abilities and personalities. The information vacuumed up by the N.S.A. was already available to faceless bureaucrats in phone and Internet companies — not government employees, but strangers just the same. Many people write as though we make some great sacrifice by disclosing private information to others, but it is in fact simply the way that we obtain services we want — whether the market services of doctors, insurance companies, Internet service providers, employers, therapists and the rest, or the nonmarket services of the government like welfare and security. Even so, I am exaggerating the nature of the intrusion. The chance that human beings in government will actually read our e-mails or check our phone records is infinitesimal (though I can understand that organizations like the A.C.L.U. that have a legitimate interest in communicating with potential government targets may be more vulnerable than the rest of us). Mostly all we are doing is making our information available to a computer algorithm, which is unlikely to laugh at our infirmities or gossip about our relationships.

4. Most of us are innocent anyway, so we have nothing to fear from the NSA programs

Richard Lempert, Professor, Law, University of Michigan, “PRISM and Boundless Informant: IS NSA Surveillance a Threat?” UP FRONT, Brookings Institution, 6—13—13, www.brookings.edu/blogs/up-front/posts/2013/06/13-prism-boundless-informant-nsa-surveillance-lempert, accessed 10-4-13.

It is easy to be cynical about government and the respect that agencies show for the laws under which they operate. Cynicism is fed by occasional scandals and by the more frequent pseudo-scandals which make it appear that within the Beltway things are out of control. Having spent four years as a Division Director at the National Science Foundation and three years as Chief Scientist in the Human Factors/ Behavioral Science Division of DHS’s Science and Technology Directorate, I am not cynical. Time and again I have seen government employees seek to follow the law even when it seems silly and interferes with their mission. When I joined DHS I was most surprised by the fierceness of efforts to comply with the U.S. Privacy Act. At times interpretations of what the Act protected were so broad as to border on the ridiculous, and costs were real: research projects with national security implications were delayed, redesigned or even precluded because privacy officers, sometimes with little basis in the statute, felt there was a risk that personally identifiable information (PII) would be impermissibly collected. The absence of any reason to fear revelation or misuse made no difference. The strict scrutiny applied to research that might involve PII is, to be sure, relaxed in front line operational settings like PRISM and legal restrictions may differ, but my experience in two agencies as well as conversations with people in the intelligence community (IC) lead me to believe that it is a mistake to regard as a sham the legal restrictions on PRISM or other IC data mining and surveillance activities. Through its PRISM and Boundless Informant efforts, NSA is working to protect the nation, apparently with some success. The 99.9% of us who pose no threat of terrorism and do not inadvertently consort with possible terrorists should not worry that the government will track our phone or internet exchanges or that our privacy will be otherwise infringed.

Surveillance Desirable: Answers to “Privacy”—General [cont’d]**5. The current NSA programs do not pose much of a privacy threat—we just need to be vigilant about the potential downside risks of future tech developments**

Richard Lempert, Professor, Law, University of Michigan, “PRISM and Boundless Informant: IS NSA Surveillance a Threat?” UP FRONT, Brookings Institution, 6—13—13, www.brookings.edu/blogs/up-front/posts/2013/06/13-prism-boundless-informant-nsa-surveillance-lempert, accessed 10-4-13.

Data mining in connection with PRISM and Boundless Informant appropriately raises concerns. But it would not be surprising if upon closer inspection and as more is known, it is discovered that the privacy threats that these programs pose for American citizens are small, their compliance with legal restrictions is genuine, and their contributions to the fight against terrorism has value more than commensurate with any costs they impose. At the same time we are well advised to be wary about what we are creating. Efforts associated with the “war against terrorism should be regarded as military in essence, and the posse comitatus law which prevents the military from acting to enforce domestic criminal law, no matter how great the need, should be clearly extended and strictly applied to the NSA, the CIA and similar organizations, including some aspects of work done by the FBI, even if they could make valuable contributions to crime control more generally. Moreover, what we are learning about these programs should serve as a wakeup call to stimulate social and political changes that will make it less likely and less possible for a government in power to extend its time in office by undemocratic means. In addition, as we think about privacy and data mining, we should be as alert to and concerned about the privacy dangers posed by private and state sector data mining as we are to the dangers posed by federal activity. Regardless of who is doing the infringing, privacy is a human value we should cherish.

Surveillance Desirable: Answers to “Privacy”—Internal Safeguards

1. The NSA programs are subject to substantial safeguards, will not be abused

Max Boot, senior fellow, Council on Foreign Relations, “Stay Calm and Let the NSA Carry On,” LOS ANGELES TIMES, 6—9—13, <http://articles.latimes.com/2013/jun/09/opinion/la-oe-boot-nsa-surveillance-20130609>, accessed 10-4-13.

Which brings us to the current kerfuffle over two NSA monitoring programs that have been exposed by the Guardian and the Washington Post. One program apparently collects metadata on all telephone calls made in the United States. Another program provides access to all the emails, videos and other data found on the servers of major Internet firms such as Google, Apple and Microsoft. At first blush these intelligence-gathering activities raise the specter of Big Brother snooping on ordinary American citizens who might be cheating on their spouses or bad-mouthing the president. In fact, there are considerable safeguards built into both programs to ensure that doesn't happen. The phone-monitoring program does not allow the NSA to listen in on conversations without a court order. All that it can do is to collect information on the time, date and destination of phone calls. It should go without saying that it would be pretty useful to know if someone in the U.S. is calling a number in Pakistan or Yemen that is used by a terrorist organizer. As for the Internet-monitoring program, reportedly known as PRISM, it is apparently limited to “non-U.S. persons” who are abroad and thereby enjoy no constitutional protections. These are hardly rogue operations. Both programs were initiated by President George W. Bush and continued by President Obama with the full knowledge and support of Congress and continuing oversight from the federal judiciary. That's why the leaders of both the House and Senate intelligence committees, Republicans and Democrats alike, have come to the defense of these activities.

2. There is no evidence that the surveillance programs are being abused

Max Boot, senior fellow, Council on Foreign Relations, “Stay Calm and Let the NSA Carry On,” LOS ANGELES TIMES, 6—9—13, <http://articles.latimes.com/2013/jun/09/opinion/la-oe-boot-nsa-surveillance-20130609>, accessed 10-4-13.

It's possible that, like all government programs, these could be abused — see, for example, the IRS making life tough on tea partiers. But there is no evidence of abuse so far and plenty of evidence — in the lack of successful terrorist attacks — that these programs have been effective in disrupting terrorist plots. Granted there is something inherently creepy about Uncle Sam scooping up so much information about us. But Google, Facebook, Amazon, Twitter, Citibank and other companies know at least as much about us, because they use very similar data-mining programs to track our online movements. They gather that information in order to sell us products, and no one seems to be overly alarmed. The NSA is gathering that information to keep us safe from terrorist attackers. Yet somehow its actions have become a “scandal,” to use a term now loosely being tossed around. The real scandal here is that the Guardian and Washington Post are compromising our national security by telling our enemies about our intelligence-gathering capabilities. Their news stories reveal, for example, that only nine Internet companies share information with the NSA. This is a virtual invitation to terrorists to use other Internet outlets for searches, email, apps and all the rest. No intelligence effort can ever keep us 100% safe, but to stop or scale back the NSA's special intelligence efforts would amount to unilateral disarmament in a war against terrorism that is far from over.

Surveillance Desirable: Answers to “Privacy”—Internal Safeguards [cont’d]

3. The metadata database is subject to tight controls and is only rarely used

Steven G. Bradbury, Dechert, LLP, Testimony before the House Judiciary Committee, 7—17—13, <http://judiciary.house.gov/hearings/113th/07172013/Bradbury%2007172013.pdf>, accessed 10-2-13.

The metadata acquired consists of the transactional information that phone companies retain in their systems for a period of time in the ordinary course of business for billing purposes and that appears on typical phone bills. It includes only data fields showing which phone numbers called which numbers and the time and duration of the calls. This order does not give the government access to any information about the content of calls or any other subscriber information, and it doesn't enable the government to listen to anyone's phone calls. Access to the data is limited under the terms of the court order. Contrary to some news reports, there's no data mining or random sifting of the data permitted. The database may only be accessed through queries of individual phone numbers and only when the government has reasonable suspicion that the number is associated with a foreign terrorist organization. If it appears to be a U.S. number, the suspicion cannot be based solely on activities protected by the First Amendment, such as statements of opinion, books or magazines read, Web sites visited, or places of worship frequented. Any query of the database requires approval from a small circle of designated NSA officers. A query will simply return a list of any numbers the suspicious number has called and any numbers that have called it and when those calls occurred. Nothing more. The database includes metadata going back five years, to enable an analysis of historical connections. Any records older than five years are continually purged from the system and deleted. In analyzing links to suspicious numbers, any connections that are found to numbers inside the United States will of course be of most interest, because the analysis may suggest the presence of a terrorist cell in the U.S. Based in part on that information, the FBI may seek a separate FISA order for surveillance of a U.S. number, but that surveillance would have to be supported by individualized probable cause. The NSA has confirmed that in all of 2012, there were fewer than 300 queries of the database, and only a tiny fraction of the data has ever been reviewed by analysts. The database is kept segregated and is not accessed for any other purpose, and FISA requires the government to follow procedures overseen by the court to minimize any unnecessary dissemination of U.S. numbers generated from the queries.

4. There is no evidence that the NSA programs have been abused

Max Boot, fellow, Council on Foreign Relations, “‘Top Secret’ Should Mean Just That,” COMMENTARY, 6—6—13, www.commentarymagazine.com/2013/06/06/top-secret-should-mean-just-that/#more-826751, accessed 10-12-13.

Now it seems to be open season on the secret intelligence-gathering programs of the U.S. government. Following the Guardian's exposure of this data-mining program that collects phone logs, the Washington Post has decided to reveal the existence of a program code-named PRISM which allows the National Security Agency to tap “into the central servers of nine leading U.S. Internet companies, extracting audio, video, photographs, e-mails, documents and connection logs that enable analysts to track a person's movements and contacts over time.” These disclosures raise obvious privacy concerns that deserve to be further explored by Congress behind closed doors. But there is no suggestion on the evidence so far presented that either program is illegal or unauthorized or that it has been misused for nefarious purposes. Quite the opposite: Mike Rogers, chairman of the House Intelligence Committee, says that the data-mining program has been used to avert at least one terrorist attack.

5. Federal agencies can only access citizen data with court approval

Karuna Chandwani, “PRISM Helped Dodge Over 50 Terror Attacks,” INTERNATIONAL BUSINESS TIMES, 6—19—13, www.ibtimes.co.in/articles/480569/20130619/nsa-chief-hearing-prism-national-security-agency.htm, accessed 10-12-13.

Alexander, the NSA director, was supported by some of the most senior intelligence officials in the House of Intelligence Committee in defending the broad surveillance programs as a vital security tool. He denied the claim by Edward Snowden, the whistleblower who leaked the NSA's surveillance program to The Guardian and Washington Post, that the NSA had the ability to 'tap into virtually any American's phone or emails'. "I know of no way to do that," said Alexander. Moreover, there were repeated assurances that none of the law enforcement agencies involved can access personal records of a US citizen without (FISA) court approval. Surrounded by senior FBI officials from the FBI, Justice Department and Office of the Director of National Intelligence, Alexander warned that the disclosure of the surveillance programs by the two international dailies could cause "a long and irreversible impact on our nation's security and on that of our allies."

Surveillance Desirable: Answers to “Privacy”—Metadata

1. Metadata searches are narrowly tailored—addresses privacy concerns

WALL STREET JOURNAL, “Thank You for Data-Mining,” 6—7—13,

<http://online.wsj.com/news/articles/SB10001424127887324299104578529373994191586>, accessed 10-12-13.

The outrage this time seems to stem from the fact that the government is widely collecting call records, not merely those associated with a particular suspect or group. But this fear misunderstands how the program works. From what we know, the NSA runs algorithms over the call log database, searching for suspicious patterns over time. refine the deviations. A nongovernment analogue might be the credit card flags that freeze payment when, say, a New Yorker goes on a shopping spree in Phoenix. The Washington Post also revealed Thursday that NSA has a parallel metadata program for Internet address packets called Blarney. If the NSA's version of a computer science department operates like the rest of FISA, the government is cautious to ensure that its searches are narrowly tailored and specific protocols are reviewed by FISA judges. Mike Rogers, the Chairman of the House Intelligence Committee, said Thursday that the program had helped disrupt a major domestic terror attack in recent years.

2. The metadata programs pose little privacy threat to innocent Americans

Richard Lempert, Professor, Law, University of Michigan, “PRISM and Boundless Informant: IS NSA Surveillance a Threat?”

UP FRONT, Brookings Institution, 6—13—13, www.brookings.edu/blogs/up-front/posts/2013/06/13-prism-boundless-informant-nsa-surveillance-lempert, accessed 10-4-13.

The NSA's recently revealed PRISM project allows the NSA to monitor the internet traffic of foreigners, but sweeps up American communicators in the process while the once equally secret Boundless Information program analyzes and is fed in part by metadata on calls routed through Verizon, and it is safe to assume, other telecommunications carriers as well. How concerned should we be? The answer depends on what one's concerns are. If the concern is the privacy of one's own conversations, there is little reason for all but a handful of Americans to lose sleep over this, and those most likely to lose sleep are also most likely to pose security threats. The programs are somewhat different, but given what we have been told so far, here's how they are likely to work. The telecommunications data mining appears to be both vast and indiscriminate but only collects so-called metadata; that is, data on which phone numbers called which other numbers, how long the calls lasted, the locations where calls were made and received and the like. No conversations have been recorded, so what was said is forever beyond the government's reach. If, however, a number called or called from belongs to a suspected terrorist, here or abroad, or to someone whose calling patterns or call locations arouse suspicions, the NSA, FBI or other agency will most likely be able to secure a warrant, based on probable cause, that will authorize listening to what is said in calls to and/or from the identified number. It is not, however, just those who call or are called by previously identified suspicious numbers who will be vulnerable to having their calls seen as suspicious and their conversations monitored. Data mining can cast suspicion on those who call others who have called suspicious numbers, those who call third party numbers whom suspicious callers call and the like. Still, although the net is potentially wide, it is likely that relatively few Americans are selected for active surveillance, and then only after a court has reviewed the reasonableness of monitoring requests given patterns in the metadata and connections to known security risks.

3. Metadata analysis is inevitable—there is nothing we can do to stop it

Paul Rosenzweig, visiting fellow, Heritage Foundation, Testimony before the Senate Subcommittee on Oversight of Government Management, the Federal Workforce and the District of Columbia Committee on Homeland Security and Governmental Affairs, 7—31—12, <http://www.heritage.org/research/testimony/2012/08/the-state-of-privacy-and-security-our-antique-privacy-rules>, accessed 10-3-13.

The growth of dataveillance is inevitable. It reflects a fundamental change caused by technological advances that, like King Canute's fabled tide, cannot be stopped or slowed. Increasingly, the cyber conflict will be fought, and won, by those who use data to their best advantage. The opportunity or problem, depending on one's perspective derives from two related, yet distinct trends: increases in computing power and decreases in data storage costs. Many are familiar with the long-term increase in the power of computers. It is most familiarly characterized as Moore's Law named after Intel computer scientist Gordon Moore, who first posited the law in 1965. Moore's Law predicts that computer chip capacities will double every eighteen to twenty-four months. Moore's law has been remarkably constant for nearly thirty years, as the graph below demonstrates.

Surveillance Desirable: Answers to “Privacy”—Minimal Intrusion

1. The NSA only reviews a very small volume of internet traffic

Hayley Peterson, “NSA Claims It only Reviews .00004 Percent of Internet Traffic on a Daily Basis,” DAILY MAIL, 8—12—13, www.dailymail.co.uk/news/article-2390604/NSA-claims-reviews-00004-percent-Internet-traffic-daily-basis.html, accessed 10-2-13.

The NSA has claimed in a publicly-released document that it only reviews .00004% of Internet traffic on a daily basis. The seven-page document, titled 'The National Security Agency: Missions, Authorities, Oversight and Partnerships,' was released late Friday. It compares the amount of Internet data that the NSA collects to the size of a dime on a basketball court. 'According to figures published by a major tech provider, the Internet carries 1,826 Petabytes of information per day. In its foreign intelligence mission, NSA touches about 1.6% of that,' the agency states. 'However, of the 1.6% of the data, only 0.025% is actually selected for review. The net effect is that NSA analysts look at 0.00004% of the world's traffic in conducting their mission - that's less than one part in a million. Put another way, if a standard basketball court represented the global communications environment, NSA's total collection would be represented by an area smaller than a dime on that basketball court.'

2. This is not an abuse of power—the NSA is collecting minimal information

WALL STREET JOURNAL, “Thank You for Data-Mining,” 6—7—13, <http://online.wsj.com/news/articles/SB10001424127887324299104578529373994191586>, accessed 10-12-13.

The real danger from this leak is the potential political overreaction. The NSA is collecting less information than appears on a monthly phone bill (no names), but Americans would worry less about the government spying on them if, for example, the Justice Department wasn't secretly spying on the Associated Press and Fox News. Or if the IRS wasn't targeting White House critics. Or if the Administration in general showed a higher regard for the law when it conflicts with its policy preferences. The liberals who spent the Bush years warning about a knock on the door at least have the virtue of consistency, if not the Republicans who are now depicting the NSA program as some J. Edgar Hoover-Bill Moyers operation to target domestic enemies. Kentucky Senator Rand Paul has already introduced the Fourth Amendment Restoration Act of 2013. Yet surveillance is more critical than ever to stopping terror attacks now that Mr. Obama has all but abolished extended interrogation and military detention and invited Congress to limit drone strikes. Amid many real abuses of power, the political temptation will be to tie data-mining into a narrative about a government out of control. Such opportunism can only weaken our counterterrorism defenses and endanger the country.

3. The NSA actually reviews only a very small part of internet traffic

James Ball, “NSA Stores Metadata of Millions of Web Users for up to a Year, Secret Files Show,” GUARDIAN, 9—30—13, <http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents>, accessed 10-2-13.

The NSA also collects enormous quantities of metadata from the fibre-optic cables that make up the backbone of the internet. The agency has placed taps on undersea cables, and is given access to internet data through partnerships with American telecoms companies. About 90% of the world's online communications cross the US, giving the NSA what it calls in classified documents a "home-field advantage" when it comes to intercepting information. By confirming that all metadata "seen" by NSA collection systems is stored, the Marina document suggests such collections are not merely used to filter target information, but also to store data at scale. A sign of how much information could be contained within the repository comes from a document voluntarily disclosed by the NSA in August, in the wake of the first tranche of revelations from the Snowden documents. The seven-page document, titled "The National Security Agency: Missions, Authorities, Oversight and Partnerships", says the agency "touches" 1.6% of daily internet traffic – an estimate which is not believed to include large-scale internet taps operated by GCHQ, the NSA's UK counterpart. The document cites figures from a major tech provider that the internet carries 1,826 petabytes of information per day. One petabyte, according to tech website Gizmodo, is equivalent to over 13 years of HDTV video. "In its foreign intelligence mission, NSA touches about 1.6% of that," the document states. "However, of the 1.6% of the data, only 0.025% is actually selected for review. The net effect is that NSA analysts look at 0.00004% of the world's traffic in conducting their mission – that's less than one part in a million."

Surveillance Desirable: Answers to “Privacy”—Other Invasions Worse

1. Online medical records are far more invasive than the NSA programs

Jonah Goldberg, American Enterprise Institute, “Civil Libertarians’ Hypocrisy,” USA TODAY, 7—8—13, <http://aei.org/article/politics-and-public-opinion/civil-libertarians-hypocrisy/>, accessed 10-3-13.

One needn't be a privacy absolutist, never mind a paranoid conspiracy theorist, to believe that this is a legitimate concern. One can even support the NSA's PRISM program and still want significant safeguards against abuse. Your medical life What I have a hard time understanding, however, is how one can get worked up into a near panic about an overreaching national security apparatus while also celebrating other government expansions into our lives, chief among them the hydrahead leviathan of the Affordable Care Act (aka ObamaCare). The 2009 stimulus created a health database that will store all your health records. The Federal Data Services Hub will record everything bureaucrats deem useful, from your incarceration record and immigration status to whether or not you had an abortion or were treated for depression or erectile dysfunction. In other words, while the NSA can tell if you searched the Web for "Viagra," the Hub will know if you were actually prescribed the medication and for how long. Yes, there are rules for keeping that information private, but you don't need security clearance or a warrant to get it. Then there's the IRS. We already have evidence of abuse there. For instance, the National Organization for Marriage, which opposes same-sex marriage, had its tax returns and private donor information leaked to the news media last year, presumably in order to embarrass Mitt Romney (he gave the group \$10,000) and others during the presidential election. And yet, worrying about NSA abuse is cast as high-minded while worrying about ObamaCare or the IRS is seen as paranoid. Why? It's just fashionable Part of the answer surely stems from the fact the progressive dream of government-guaranteed health care is fashionable, while opposition to it is perceived by liberal elites as backward or villainous. But it goes deeper than that. There are basically two visions of oppressive government, the Orwellian and the Huxleyan. In George Orwell's 1984, the dystopia is a totalitarian police state, where everyone is snooped on and bullied. In Aldous Huxley's Brave New World, most people are happy because the government takes care of them. Culturally, Americans of all stripes recoil at anything that seems like a step on the slippery slope toward the Orwellian state. But we lack the same reflexive response against things that smack of the Huxleyan.

2. Private data collection is a far greater threat to our privacy

Sebastian Rotella, Pulitzer Prize winning journalist, “How the NSA’s High-Tech Surveillance Helped Europeans Catch Terrorists,” PROPUBLICA, 6—19—13, www.propublica.org/article/how-the-nas-high-tech-surveillance-helped-europeans-catch-terrorists, accessed 10-4-13.

The U.S. reaction to NSA data mining strikes my European interlocutors as somewhat academic — a debate about potential rather than actual abuse. They don't see a scandal. “Something that is more dangerous to individual liberties and data protection than the secret American metadata programs, such as Echelon or PRISM,” said Bruguière, “is the insufficiently controlled commercial availability of innovative technological products such as social networks or the Google Earth and Google Street programs, which can be easily diverted toward criminal or terrorist ends.” Some here see quite another problem: They think the U.S. intelligence community has overreacted to Islamic terrorism, acting as if the networks have the dimensions and discipline of Cold War-era state adversaries. That can cause excessive rigidity and secrecy.

3. Private companies do similar metadata analysis all the time

WALL STREET JOURNAL, “Thank You for Data-Mining,” 6—7—13, <http://online.wsj.com/news/articles/SB10001424127887324299104578529373994191586>, accessed 10-12-13.

The critics nonetheless say the NSA program is a violation of privacy, or illegal, or unconstitutional, or all of the above. But nobody's civil liberties are violated by tech companies or banks that constantly run the same kinds of data analysis. We bow to no one in our desire to limit government power, but data-mining is less intrusive on individuals than routine airport security. The data sweep is worth it if it prevents terror attacks that would lead politicians to endorse far greater harm to civil liberties. The program was blessed by Congress in the Patriot Act and its later amendments, with broad powers for the NSA to obtain and monitor "any tangible things" including "records, papers, documents, and other items" in order to "protect against international terrorism." As for the Fourth Amendment's ban on unreasonable searches, the Supreme Court has long held (Smith v. Maryland, 1979) that there is no legitimate expectation of privacy for phone records that are held by a third party, which can be seized without a warrant.

Surveillance Desirable: Answers to “Privacy”—Oversight Solves

1. We will be able to use the same metadata techniques to ensure that government agencies do not abuse the data they are gathering

Paul Rosenzweig, visiting fellow, Heritage Foundation, Testimony before the Senate Subcommittee on Oversight of Government Management, the Federal Workforce and the District of Columbia Committee on Homeland Security and Governmental Affairs, 7—31—12, <http://www.heritage.org/research/testimony/2012/08/the-state-of-privacy-and-security-our-antique-privacy-rules>, accessed 10-3-13.

Second, and perhaps most significantly, the very same dataveillance systems that are used to advance our counter-terrorism interests are equally well suited to assure that government officials comply with the limitations imposed on them in respect of individual privacy. Put another way, the dataveillance systems are uniquely well equipped to watch the watchers, and the first people who should lose their privacy are the officials who might wrongfully invade the privacy of others. Indeed, there are already indications that these strong audit mechanisms are effective. Recall the incident in the last presidential campaign in which contractors hacked Barack Obama’s passport file. In this instance, there was no lawful reason for the disclosure of the file; it was disclosed purely for prurient, political reasons. As a result, candidate Obama suffered an adverse consequence of disclosure which had not met any legal trigger that would have permitted the disclosure. A strong audit function quickly identified the wrongdoers and allowed punitive action to be taken. We can, therefore, be reasonably confident that as we move forward in establishing a consequence-based system of privacy protection we are also moving toward a point where the legal structures and technological capabilities to support that system are being put into place.

2. NSA searches are governed by judges—no real privacy threat

Stewart Baker, former Assistant Secretary for Policy, Department of Homeland Security, “Why the NSA Needs Your Phone Calls,” FOREIGN POLICY, 6—6—13, www.foreignpolicy.com/articles/2013/06/06/why_the_nsa_needs_your_phone_calls, accessed 10-12-13.

Suddenly, the national security establishment is drowning in data. On June 5, the Guardian released what appears to be a highly classified order issued by the Foreign Intelligence Surveillance Court, known as the FISA Court, to collect Verizon customers’ phone records of calls made to or by Americans. On June 6, the Washington Post revealed the existence of PRISM, which allows the collection of Internet data on a massive scale. Does this mean the end of privacy, law, and the Constitution? Nope. There are a lot of reasons to be cautious about rushing to the conclusion that these “scandals” signal a massive, lawless new intrusion into Americans’ civil liberties. Despite this apparent breadth, and even if we assume that the leaked FISA order is genuine, there are a lot of reasons to be cautious about rushing to the conclusion that it signals a massive, lawless new intrusion into Americans’ civil liberties. Let’s start with the order. It seems to come from the court established to oversee intelligence gathering that touches the United States. Right off the bat, that means that this is not some warrantless or extrastatutory surveillance program. The government had to convince up to a dozen life-tenured members of the federal judiciary that the order was lawful. You may not like the legal interpretation that produced this order, but you can’t say it’s lawless.

3. No abuses are likely—the program is subject of checks and balances

William Saletan, “Stop Freaking out about the NSA,” SLATE, 6—6—13, www.slate.com/articles/news_and_politics/frame_game/2013/06/stop_the_nsa_surveillance_hysteria_the_government_s_scrutiny_of_verizon.html, accessed 10-12-13.

You don’t need a wiretap to hear what people are saying about the National Security Agency’s phone surveillance program. The program’s details, disclosed in a secret court order leaked to the Guardian, show that at least one major company, Verizon, has been legally required to give the government information about its subscribers’ communications. “An astounding assault on the Constitution,” says Rand Paul. “Obscenely outrageous,” says Al Gore. “Beyond Orwellian,” says the ACLU. Chill. You can quarrel with this program, but it isn’t Orwellian. It’s limited, and it’s controlled by checks and balances. The program’s purpose, according to administration officials and knowledgeable members of Congress, is to find out who’s been calling or receiving calls from phone numbers linked to known or suspected terrorists. If Tamerlan Tsarnaev had been in contact with somebody flagged as a possible jihadist operative, this is the kind of surveillance that would have brought him to the attention of counterterrorism investigators, even without Russian assistance.

Surveillance Desirable: Answers to “Privacy”—Oversight Solves [cont’d]**4. The surveillance programs work and are subject to strict oversight**

Steven Nelson, “NSA Director: Surveillance Stopped 50 Terror Plots,” U.S. NEWS & WORLD REPORT, 6—18—13, www.usnews.com/news/newsgram/articles/2013/06/18/nsa-director-surveillance-stopped-50-terror-plots, accessed 10-2-13. Alexander, the NSA director, testified that the programs, which were unknown to the public until earlier this month, are "subject to rigorous oversight" and touted the agency's "rigorous training programs" for analysts. Under the phone record-collection program, which has been used to gather the metadata of customer phone calls from major U.S. companies for seven years, the secret Foreign Intelligence Surveillance Court requires that companies hand over records on an ongoing daily basis. The information is retained by the NSA for analysis. The orders are reissued every 90 days. Alexander lavished praise on the FISA court – where targets do not have defense attorneys present – for its "superb" job with the secret programs. "They have been extremely professional, there is, from my perspective, no rubber stamp," he said. "This is not a program that's off the books," testified Deputy Attorney General James Cole, who complained that news reports did not mention limitations on how the information can be used. Requests for access to the logs and records of access history are documented and audited, he said. Cole said the Fourth Amendment – which protects Americans from unreasonable search and seizure – does not protect the phone records of Americans because customers of phone companies do not have a reasonable expectation of privacy for records of who they call. Nonetheless, he said, American citizens and permanent residents do not have their phone logs whimsically searched.

Surveillance Desirable: Answers to “Privacy”—Section 215-Specific

1. Section 215 surveillance is legal—we have no expectation of phone metadata privacy

Carrie F. Cordero, Director, National Security Studies and Adjunct Professor of Law, Georgetown University, Testimony before the Senate Judiciary Committee, 10—2—13, <http://www.judiciary.senate.gov/pdf/10-2-13CorderoTestimony.pdf>, accessed 10-8-13.

With respect to the metadata collection under section 215, it is a fair characterization that this program is large in scale. And reasonable minds can and do disagree about whether its interpretations of relevance under the statute, or reasonableness under the Fourth Amendment, are overly broad. But I would submit that the Government’s arguments in this case are consistent with existing precedent, no matter what direction the courts may go in the future. Current Supreme Court precedent still holds that there is no expectation of privacy in our telephone metadata, that is, the numbers we dial or the numbers that dial us. A warrant is not required to obtain this information. Likewise, Supreme Court precedent also still holds that we do not have a reasonable expectation of privacy in records voluntarily turned over to a third party. The legal justification, both statutory and constitutional, is outlined in the Administration’s White Paper dated August 9, 2013.

2. The metadata program is legal under section 215—it is necessary for ongoing counterterrorism investigations

Steven G. Bradbury, Dechert, LLP, Testimony before the House Judiciary Committee, 7—17—13, <http://judiciary.house.gov/hearings/113th/07172013/Bradbury%2007172013.pdf>, accessed 10-2-13.

Now let me address the statutory and constitutional standards applicable to the acquisition of this telephone metadata. Section 215 permits the acquisition of business records that are “relevant to an authorized investigation.” Here, the telephone metadata is “relevant” to counterterrorism investigations because the use of the database is essential to conduct the link analysis of terrorist phone numbers described above, and this type of analysis is a critical building block in these investigations. In order to “connect the dots,” we need the broadest set of telephone metadata we can assemble, and that’s what this program enables. The legal standard of relevance in section 215 is the same standard used in other contexts. It does not require a separate showing that every individual record in the database is “relevant” to the investigation; the standard is satisfied if the use of the database as a whole is relevant. As I’ve indicated, the acquisition of this data and the creation and use of this database are not only relevant to ongoing counterterrorism investigations; they’re necessary to those investigations, because they offer the only means to conduct the critical analysis that provides links to new phone numbers used by agents of foreign terrorist organizations.

Surveillance Desirable: Answers to “Privacy”—Section 702-Specific

1. Section 702 data collection is used for foreign surveillance, cannot be targeted at U.S. citizens

Tim Worstall, “NSA’s PRISM Sounds Like a Darn Good Idea to Me,” FORBES, 6—7—13, www.forbes.com/sites/timworstall/2013/06/07/nsas-prism-sounds-like-a-darn-good-idea-to-me-this-is-what-governments-are-for/, accessed 10-2-13.

Whether the claim of direct access is true or not is one thing. But the much larger point is that this sort of behaviour is not something that we should be shouting about government doing. It’s something that we should be shouting about government not doing. The crucial point is here, from the DNI: Section 702 is a provision of FISA that is designed to facilitate the acquisition of foreign intelligence information concerning non-U.S. persons located outside the United States. It cannot be used to intentionally target any U.S. citizen, any other U.S. person, or anyone located within the United States. As I say that’s the important part of it all. The information, the data, may be in the US as a result of the global spread of the internet and the physical location of servers. But the information cannot be about either a US citizen or someone who is in the US. And, if we’re prepared to be honest about matters, we do actually want the government to be keeping an eye on foreigners in foreign lands. Which is what they’re doing. Take a step back for a moment. The purpose of the State, the first job it is tasked with, is the protection of that State from external enemies. This is the first principle of even having a State in the first place: to make sure that the populace is protected from the depredations of the foreigners who would do them harm. So the idea that the spies would be attempting to look at the telecoms data of said foreigners shouldn’t really surprise us. Indeed, this is something we actually want said State to be doing: this is rather the purpose of having both it and the spies it employs. The matter is entirely different when such a State uses the same methods to look at its own citizens: this is a gross abuse of power and a serious threat to any form of liberty or freedom. Which is why there are legal protections against it in most free and liberal states. And as we can see with PRISM those safeguards are in place. Data on US citizens or residents might be collected but only as a by-product of collecting it on those foreigners. Who do not have any of those legal or constitutional protections.

2. Section 702 surveillance is targeted at non-U.S. citizens, does not raise constitutional concerns

Carrie F. Cordero, Director, National Security Studies and Adjunct Professor of Law, Georgetown University, Testimony before the Senate Judiciary Committee, 10—2—13, <http://www.judiciary.senate.gov/pdf/10-2-13CorderoTestimony.pdf>, accessed 10-8-13.

Section 702 collection is targeted against non-U.S. persons reasonably believed to be outside the United States. These are not individuals with Constitutional protections, and the collection against them is conducted in accordance with the statutory framework passed by Congress in the FISA Amendments Act of 2008. The FISA Amendments Act enhanced protections for U.S. persons worldwide by requiring that an individual probable cause-based order be obtained from the FISC for electronic surveillance or physical search no matter where in the world that U.S. person is located. The minimization procedures governing 702 collection have now been declassified, and demonstrate the detailed procedures with which the NSA handles U.S. person information. The 702 framework was debated extensively and publicly, and members of this Committee have been kept informed of its implementation in accordance with the reporting provisions of FISA.

3. Section 702 searches are legal, pass constitutional muster

Steven G. Bradbury, Dechert, LLP, Testimony before the House Judiciary Committee, 7—17—13, <http://judiciary.house.gov/hearings/113th/07172013/Bradbury%2007172013.pdf>, accessed 10-2-13.

Any foreign intelligence surveillance that is targeted at a particular U.S. person or any person believed to be in the United States requires a traditional individualized FISA order supported by probable cause. Like the business records provision of FISA, section 702 goes beyond the baseline protections of the Fourth Amendment. Federal courts have consistently held that the Constitution permits the executive branch to conduct intelligence surveillance within the United States without court involvement, provided the surveillance is focused on foreign threats. See, e.g., *United States v. Truong Dinh Hung*, 629 F.2d 908, 914 (4th Cir. 1980). By establishing a detailed procedure for court approval and congressional oversight, section 702 therefore provides a system of foreign intelligence surveillance that is more restrictive than the Constitution would otherwise require. The PRISM Internet collection is precisely the type of court-approved foreign-targeted intelligence surveillance that Congress intended to authorize when it enacted and reauthorized section 702 by overwhelming majorities. This program is subject to extensive reviews and periodic reports to Congress by inspectors general, in addition to the oversight of the FISA judges. Moreover, I understand that in advance of the reauthorization of section 702 in 2012, the leaders and full membership of the Intelligence Committees of both Houses of Congress were briefed on the classified details of this program and all members of Congress were offered the opportunity for such a briefing.

Surveillance Undesirable: Topshelf

1. Surveillance schemes threaten First and Fourth Amendment rights and threaten our system of checks and balances—destroys the basis of all our other rights

Kate Martin, Center for National Security Studies, Testimony before the House Judiciary Committee, 7—17—13, <http://judiciary.house.gov/hearings/113th/07172013/Martin%2007172013.pdf>, accessed 10-2-13.

I want to raise two overarching concerns for this Committee's consideration during the current debate, which I hope will inform your consideration of necessary oversight measures as well as specific changes to the statutory language. First, we are concerned that the unprecedented massive collection of information on Americans, the creation of secret databanks which are available for government analysis, queries, and data-mining by ever increasingly sophisticated computerized tools, and the dissemination of both raw information and the results of such analysis or data-mining throughout the executive branch pose unprecedented threats to First and Fourth Amendment liberties. Second, the secrecy that surrounds this government surveillance – not of foreign governments or other foreign targets – but of Americans – poses a significant and perhaps unprecedented challenge to our system of constitutional checks and balances. It has long been recognized as Senator Sam Ervin, the author of the Privacy Act put it in 1974: “[D]espite our reverence for the constitutional principles of limited Government and freedom of the individual, Government is in danger of tilting the scales against those concepts by means of its information gathering tactics and its technical capacity to store and distribute information. When this quite natural tendency of Government to acquire and keep and share information about citizens is enhanced by computer technology and when it is subjected to the unrestrained motives of countless political administrators, the resulting threat to individual privacy makes it necessary for Congress to reaffirm the principle of limited, responsive Government on behalf of freedom. Each time we give up a bit of information about ourselves to the Government, we give up some of our freedom: the more the Government or any institution knows about us, the more power it has over us. When the Government knows all of our secrets, we stand naked before official power. Stripped of our privacy, we lose our rights and privileges. The Bill of Rights then becomes just so many words.” Senator Sam Ervin, June 11, 1974, reprinted in Committee On Government Operations, United States Senate And The Committee On Government Operations, House Of Representatives, Legislative History Of The Privacy Act Of 1974, S.3418, at 157 (Public Law 93-579)(Sept. 1976).

2. Violations of privacy are such that the impact of the whole may be worse than the sum of its parts

G. Alex Sinha, fellow, Human Rights Watch, “NSA Surveillance Since 9/11 and the Human Right to Privacy,” LOYOLA LAW REVIEW, 8—31—13, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2327806, accessed 10-12-13.

Violations of other rights manifest differently. A right not to be detained arbitrarily is only violated once each time I am detained that way, regardless of how many people sign off on the decision to hold me. Even in a state that widely detains people arbitrarily, the number of violations of the right to be free from such treatment will simply never threaten to approach the number of potential privacy violations that could occur in a state that widely conducts illegal surveillance on its people. That is just a feature of what the right protects against, and thus the ways in which it can be violated. The number of violations and the seriousness of each violation are largely independent, but privacy introduces an interesting wrinkle here. If the NSA improperly collects enough data points about me, the seriousness of the total harm to me could transcend the seriousness of the harm to me from the collection of each individual piece of information. That is, the whole harm could be greater than the sum of its parts. A distinct fact in isolation may not reveal a great deal that is private about me, but a collection of information detailed enough to expose further information by implication or by the interaction of its individual data points could reveal exponentially more. In cases where many violations result from the improper storage and review of a single email, perhaps we will find the large total number of violations misleading to the extent that we are naturally primed to infer greater harm from it. But in cases where the large number of violations involves the assembly and deployment of data to create detailed pictures of people's activities and preferences, the large number of violations may actually understate the harm. Some of these features of the right to privacy may be helpful in considering the ways in which the ICCPR might prohibit (parts of) the NSA program.

Surveillance Undesirable: Topshelf [cont'd]

3. ‘Total surveillance’ threatens democracy and liberty

Danielle Keats Citron and David Gray, University of Maryland School of Law, “Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards,” *HARVARD LAW REVIEW FORUM* v. 126, 2013, p. 268-269.

Rather than assigning primary edged perils of broader types of surveillance, the law’s focus should be on the dangers of totalizing surveillance. Information privacy scholars and surveillance studies theorists alike have long adhered to this approach, and for good reason. Technologies like Virtual Alabama and the fusion-center network amass, link, analyze, and share mass quantities of information about individuals, much of which is quotidian. What is troubling about these technologies is not what information they gather, but rather the broad, indiscriminate, and continuous nature of the surveillance they facilitate. Video cameras may be trained on street corners, drugstore aisles, or a school’s bathroom en-trances. The information they gather likely does not implicate intellectual activities. They nonetheless create and sustain the kind of surveillance state that is anathema to liberty and democratic culture. Fusion centers rely upon data-broker dossiers, much of which has nothing to do with intellectual endeavors. There is no doubt, however, that continuously streaming all of this information into the information-sharing environment facilitates the sort of broad and indiscriminate surveillance that is characteristic of a surveillance state.

4. Even if the intent is not totalitarian, the program itself enables it

Jonathan Schell, fellow, The Nation Institute, “Edward Snowden and Chelsea Manning, the New Dissidents?” *THE NATION*, 9—4—13, <http://www.thenation.com/article/176032/edward-snowden-and-chelsea-manning-new-dissidents>, accessed 10-3-13.

And certainly, the four Poles, of all people, are as fully aware as any sensible person of the abyss of difference that separates the Obama administration from, say, the regime of Joseph Stalin, slayer of tens of millions of his own people. And yet it is chillingly true at the same time that the US government has gone further than any previous government—not excluding Stalin’s—in setting up machinery that satisfies certain tendencies that are in the genetic code of totalitarianism. One is the ambition to invade personal privacy without check or possibility of individual protection. This was impossible in the era of mere phone wiretapping, before the recent explosion of electronic communications—before the cellphones that disclose the whereabouts of their owners, the personal computers with their masses of personal data and easily penetrated defenses, the e-mails that flow through readily tapped cables and servers, the biometrics, the street-corner surveillance cameras. But now, to borrow the name of an intelligence program from the Bush years, “Total Information Awareness” is technologically within reach. The Bush and Obama administrations have taken giant strides in this direction. That China and Russia—and Britain, and many other countries—have done the same is hardly comforting to the humble individual under the eye of the universal spying apparatus. A second totalitarian tendency has been the ambition to control the entire globe—a goal built into fascist as well as communist ideologies of the early twentieth century. In Hannah Arendt’s words, “Evidence that totalitarian governments aspire to conquer the globe and bring all countries on earth under their domination can be found repeatedly in Nazi and Bolshevik literature.” Neither achieved it, or even came close. But now, in the limited arena of information, a sort of shadow or rudiment of this ambition is near realization by the “sole superpower,” the United States. Much attention has been paid to Americans’ loss of privacy rights, but relatively overlooked in the debate over the government’s surveillance activities (at least in the United States) has been that all foreign communications—including those occurring in the lands of close allies, such as Germany—are fair game and are being swept into the US data banks. The extent of the US global reach over information was mirrored in Snowden’s fate. Astonishingly, almost no fully democratic country would have him. (The conspicuous exception was Bolivia, whose president suffered the indignity of a forced diversion and landing of his plane when he was suspected of carrying Snowden to safety.) Almost all others, including Poland, bowed to US pressure, actual or potential, to refuse Snowden protection. The Polish letter writers were scandalized by this spectacle. “The fact that only dictatorial governments agreed to give him shelter shames the democratic states,” they wrote. “Our democracies discredit themselves with their indifference and cowardice in this matter.” What happened to Snowden in Moscow diagramed the new global reality. He wanted to leave Russia, but the State Department, in an act of highly dubious legality, stripped him of his passport, leaving him—for purposes of travel, at least—stateless. Suddenly, he was welcome nowhere in the great wide world, which shrank down to a single point: the transit lounge at Sheremetyevo. Then, having by its own action trapped him in Russia, the administration mocked and reviled him for remaining in an authoritarian country. Only in unfree countries was Edward Snowden welcome. What we are pleased to call the “free world” had become a giant prison for a hero of freedom.

Surveillance Undesirable: Topshelf [cont'd]

5. The NSA is subject to dangerous ‘mission creep’ and the data is likely to be used by other agencies—our entire lives risk become surveilled

Alex Abdo, Staff Attorney, ACLU National Security Project, “Latest FISA Court Opinion: A Preview of Surveillance without Limits,” FREE FUTURE, American Civil Liberties Union, 9—18—13, <https://www.aclu.org/blog/national-security/latest-fisa-court-opinion-preview-surveillance-without-limits>, accessed 10-8-13.

This should trouble us all for another reason: mission creep. The NSA’s surveillance is not limited to suspected terrorists. In fact, the government defines its “foreign intelligence” mission extraordinarily broadly to include gathering information about “foreign affairs.” And surveillance doesn’t stop with the NSA. Other agencies have already clamored for access to the NSA’s vast databases, and there’s little to stop the government from attempting to import the FISC’s sweeping surveillance logic into other areas. I’m sure it would be useful to the FBI in investigating health-care fraud to have every American’s medical records, or in investigating drug conspiracies to have all of our telephony and email metadata, or in investigating illegal gun sales to have a record of every gun sale. As our private lives become even more digitized, the lure of our data will become irresistible to the intelligence agencies. Historically, we have resisted that Orwellian urge by adhering to two key principles enshrined in our Constitution: that the government’s surveillance be targeted and that it be approved in advance by a court on an individualized basis. The NSA has subverted those essential safeguards against pervasive surveillance.

6. Spying won’t work—spurs a global reaction/backlash that confounds surveillance efforts

Martha Mendoza, “Backlash Grows to NSA Surveillance,” ASSOCIATED PRESS, 10—13—13, http://www.denverpost.com/nationworld/ci_24297907/backlash-grows-nsa-surveillance, accessed 10-14-13.

From Silicon Valley to the South Pacific, counterattacks to revelations of widespread National Security Agency surveillance are taking shape, from a surge of new encrypted e-mail programs to technology that sprinkles the Internet with red-flag terms to confuse would-be snoopers. Policymakers, privacy advocates and political leaders around the world have been outraged at the near weekly disclosures from former intelligence contractor Edward Snowden that expose sweeping U.S. government surveillance programs. “Until this summer, people didn’t know anything about the NSA,” said Amy Zegart, co-director of the Center for International Security and Cooperation at Stanford University. “Their own secrecy has come back to bite them.” Activists are fighting back with high-tech civil disobedience, entrepreneurs want to cash in on privacy concerns, Internet users want to keep snoopers out of their computers and lawmakers want to establish stricter parameters. Some of the tactics are more effective than others. For example, Flagger, a program that adds words like “blow up” and “pressure cooker” to web addresses that users visit, is probably more of a political statement than actually confounding intelligence agents. Developer Jeff Lyon in Santa Clara, Calif., said he is delighted if it generates social awareness, and that 2,000 users have installed it to date. He said, “The goal here is to get a critical mass of people flooding the Internet with noise and make a statement of civil disobedience.” University of Auckland associate professor Gehan Gunasekara said he has received “overwhelming support” for his proposal to “lead the spooks in a merry dance,” visiting radical websites and setting up multiple online identities. And “pretty soon everyone in New Zealand will have to be under surveillance,” he said. Electronic Frontier Foundation activist Parker Higgins in San Francisco has a more direct strategy: by using encrypted e-mail and browsers, he creates more smoke screens for the NSA. “Encryption loses its value as an indicator of possible malfeasance if everyone is using it,” he said. CryptoParties are springing up around the world as well. They are small gatherings where hosts teach attendees, who bring their digital devices, how to download and use encrypted e-mail and secure Internet browsers. “Honestly, it doesn’t matter who you are or what you are doing. If the NSA wants to find information, they will,” said organizer Joshua Smith. “But we don’t have to make it easy for them.”

Surveillance Undesirable: Topshelf [cont'd]

7. Accountability is impossible with the current program—resistant to congressional oversight, secrecy checks public scrutiny

American Civil Liberties Union, “United States’ Compliance with the International Covenant on Civil and Political Rights,” SHADOW REPORT TO THE FOURTH PERIODIC REPORT OF THE UNITED STATES, 9—13—13, p. 48.

The Foreign Intelligence Surveillance Act (FISA) affords the government sweeping power to monitor the communications of innocent people, and the law’s imposition of excessive secrecy over the existence, operation, and oversight of the programs it authorizes has made legislative oversight difficult and public oversight impossible. Intelligence officials have repeatedly misled the public, the U.S. Congress, and domestic courts about the nature and scope of the government’s surveillance activities. Moreover, structural features of the Foreign Intelligence Surveillance Court (FISC) have changed dramatically since the court was first established more than thirty years ago, and it is clear from recent disclosures that those changes prevent that court from serving as an effective guardian of individual rights and overseer of executive power. Finally, challenges to the U.S. government’s surveillance practices in regular U.S. courts have been thwarted by procedural doctrines that foreclose meaningful and substantive judicial review of U.S. government surveillance programs, enabling the executive branch to act, improperly and inadequately, as its own “check.”

8. Even the PATRIOT Act’s author has disavowed the NSA program

Paul M. Barrett, “NSA Surveillance Makes for Strange Bedfellows,” BUSINESSWEEK, 9—7—13, www.businessweek.com/articles/2013-09-07/nsa-surveillance-makes-strange-bedfellows, accessed 10-10-13.

Now one of the lead authors of the Patriot Act has joined the ACLU in a “friend of the court” brief (PDF). Representative James Sensenbrenner (R-Wis.), represented by the Electronic Frontier Foundation, another civil liberties nonprofit group, contends that “the unfocused dragnet undertaken by [the NSA] is exactly the type of unrestrained surveillance” Congress intended to prevent. The vast majority of the records collected, the brief adds, “will have no relation to the investigation of terrorism at all.” Having an architect of the Patriot Act disavow the NSA’s interpretation of the statute would seem like a devastating blow to the spy agency’s collection of phone numbers, call times, and other information. (The government insists that it actually listens to what people are saying only in connection with specific national security investigations.)

Surveillance Undesirable: Chilling Effect

1. The threat of chilling is real—even thinking that we are being watched for cause people to limit their activities

Jameer Jaffer, fellow, Open Society Foundations, “Secrecy and Freedom,” NEW YORK TIMES, Room for Debate, 6—9—13, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined>, accessed 10-4-13. You say you are unaware of a single instance, since 9/11, in which the government used surveillance to target a political opponent, dissenter or critic. But if the government were using surveillance this way, would officials tell us? So much secrecy surrounds the government’s surveillance activities that we simply don’t know how often, or in what ways, the government’s surveillance powers have been abused. This said, we know enough that we ought to be worried. Here is an article about the Department of Homeland Security conducting inappropriate surveillance of protesters associated with Occupy Wall Street. Here is a report of the Justice Department’s inspector general finding that the F.B.I. monitored a political group because of its anti-war views. Here is a story in which a former C.I.A. official says that the agency gathered information about a prominent war critic “in order to discredit him.” These abuses are real, but if we focus on them exclusively we risk overlooking the deeper implications of pervasive government surveillance. When people think the government is watching them, or that it might be, they become reluctant to exercise democratic freedoms. They may be discouraged from visiting officially disfavored Web sites, joining controversial political groups, attending political rallies or criticizing government policy. This is a cost to the people who don’t exercise their rights, but it’s a cost to our society, too. The chilling effect of surveillance makes our public debates narrower and more inhibited and our democracy less vital. This is the greater threat presented by the kinds of programs that were exposed this past week.

2. The gathered information threatens our democratic form of government—chills dissent

Kate Martin, Center for National Security Studies, Testimony before the House Judiciary Committee, 7—17—13, <http://judiciary.house.gov/hearings/113th/07172013/Martin%2007172013.pdf>, accessed 10-2-13. As others have detailed, there are serious questions whether these bulk collection programs are within the intended statutory authorizations, e.g., the domestic telephony meta-data program under sec. 215. There are serious constitutional concerns about the breadth of and lack of individualized suspicion or particularity in these programs. And there are serious questions whether the secrecy built into the programs is constitutional and whether it is consistent with effective oversight or a working system of checks and balances. In examining these authorities and programs, it is important to review not only whether private information about Americans held in government databases is adequately protected from rogue employees or contractors stealing or misusing the information. While safeguards are needed against that kind of privacy abuse, the more important danger is that there are inadequate safeguards against government violations of the law or against deliberate misuse of the information to target the government’s political opponents, chill dissent or unconstitutionally profile minority communities. As the original Framers recognized, all governments may succumb to the temptations of power. In my lifetime Senator McCarthy smeared civil servants, the FBI tried to blackmail Dr. Martin Luther King in order to weaken the civil rights movement, President Nixon created an enemies list of his political opponents, and the Justice Department wrote a secret legal opinion that the President could break the law in secret if he deemed it necessary for national security.

3. Surveillance systems threaten our “intellectual privacy”—threatens our free expression

Danielle Keats Citron and David Gray, University of Maryland School of Law, “Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards,” HARVARD LAW REVIEW FORUM v. 126, 2013, p. 266. Richards is right to call for the protection of “intellectual privacy.” Reflecting his concerns, the U.S. Senate’s Permanent Subcommittee on Investigations recently reported internal Department of Homeland Security warnings about agents routinely using fusion centers to collect intelligence on “First Amendment-protected activities lacking a nexus to violence or criminality,” including those of religious and political groups. One fusion center instructed law enforcement to collect information on supporters of third-party candidates, including the public movements of cars with bumper stickers supporting Ron Paul and Bob Barr. Expressing the impact of this sort of surveillance on intellectual privacy, one political activist explained that he feared being pulled over by a police officer because of political views expressed by his bumper sticker. Although much fusion center surveillance remains hidden, Richards’s concerns are valid and pressing; in the present, as in the past, there can be no doubt that surveillance systems interfere with expressive activities.

Surveillance Undesirable: Chilling Effect [cont'd]

4. Metadata collection violates the First Amendment—chills speech

Jameel Jaffer, Deputy Legal Director, ACLU Foundation and Laura W. Murphy, Director, Washington Legislative Office, ACLU, Testimony before the House Judiciary Committee, 7—17—13, <http://judiciary.house.gov/hearings/113th/07172013/Jaffer%2007172913.pdf>, accessed 10-2-13.

Because the metadata program vacuums up sensitive information about associational and expressive activity, it is also unconstitutional under the First Amendment. The Supreme Court has recognized that the government's surveillance and investigatory activities have an acute potential to stifle association and expression protected by the First Amendment. See, e.g., *United States v. U.S. District Court*, 407 U.S. 297 (1972). As a result of this danger, courts have subjected investigatory practices to —exacting scrutiny□ where they substantially burden First Amendment rights. See, e.g., *Clark v. Library of Congress*, 750 F.2d 89, 94 (D.C. Cir. 1984) (FBI field investigation); *In re Grand Jury Proceedings*, 776 F.2d 1099, 1102-03 (2d Cir. 1985) (grand jury subpoena). The metadata program cannot survive this scrutiny. This is particularly so because all available evidence suggests that the program is far broader than necessary to achieve the government's legitimate goals. See, e.g., Press Release, Wyden, Udall Question the Value and Efficacy of Phone Records Collection in Stopping Attacks, June 7, 2013, <http://1.usa.gov/19Q1Ng1> (—As far as we can see, all of the useful information that it has provided appears to have also been available through other collection methods that do not violate the privacy of law-abiding Americans in the way that the Patriot Act collection does.”).

Surveillance Undesirable: Cybersecurity

- **Spying threatens cybersecurity—makes companies reluctant to cooperate with the NSA, leaving our infrastructure vulnerable**

Aliya Sternstein, "Industry Backlash against Surveillance Jeopardizes Cybersecurity," NEXTGOV, 9—5—13, www.nextgov.com/cybersecurity/2013/09/industry-backlash-against-surveillance-jeopardizes-cybersecurity/69940/, accessed 10-11-13.

The private sector's distrust of the National Security Agency following domestic spying revelations could undermine efforts to secure systems running utilities and other vital U.S. industries, former federal civilian and military officials say. NSA, maker of arguably the best encryption tools to protect data, now is attracting more attention for decrypting everyone else's data, after disclosures by ex-NSA contractor Edward Snowden of massive Internet surveillance. "NSA has postured itself as a neutral arbiter who could provide these capabilities to the private sector and really didn't necessarily want much in return," said Christopher Finan, a former White House and Pentagon official who, until July, was involved in a Defense Department cyber offense research program called Plan X. "I don't know if they can present themselves as the same honest broker now that we're seeing the enormous quantities of data that they are actually taking in." Traditionally, private industry has counted on NSA's cybersecurity expertise for incident response, even though a 2003 presidential directive assigned the Homeland Security Department the primary job of securing key U.S. sectors. Now, many of those critical infrastructure firms might shun any government help, former officials said. Going forward, private cyber forensics firms and nonprofit research institutes could see increased demand. "Part of the fallout from the NSA revelations is that the private sector has somewhat less confidence in government to manage its information and its networks. I think that neither DHS nor DoD grow in stature in the eyes of industry because government, generally, is viewed with increased scrutiny," said Alec Ross, a former senior State Department Internet policy adviser for the Obama administration. He added, "Ironically, any decreased confidence in government by industry comes in no small measure because of wariness of government contractors. The fact that such a screwed up kid as Edward Snowden was able to access extremely sensitive content does not build confidence." James Lewis, a fellow at the Center for Strategic and International Studies who advises agencies and Congress on cybersecurity, said there definitely will be reluctance to turn to NSA for protection -- and that is unfortunate. The degree of government involvement in regulating cybersecurity and facilitating the exchange of information about threats will remain status quo, he said. "If anything we're just a little further back because NSA playing a larger role is definitely out of the question, but that doesn't mean that we'll do something else. It just that it means that we'll do less of what we're doing now."

Surveillance Undesirable: Democracy

1. Secrecy about government policy is dangerous, is corrosive to our democracy

Jameer Jaffer, fellow, Open Society Foundations, “Secrecy and Freedom,” NEW YORK TIMES, Room for Debate, 6—9—13, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined>, accessed 10-4-13.

Your claim about the pervasiveness and banality of government secrecy elides the fact that there are many kinds of secrecy. Not all of them present the same threat to democracy. I don’t think our democracy is made weaker by the government’s withholding of information about the technical means it uses to effect surveillance. I don’t think our democracy is made weaker by the government’s withholding of information about the specific targets of its surveillance — so long as the surveillance is in fact limited to specific targets and so long as there is some mechanism that permits the public to evaluate the government’s conduct after the investigation is complete. Secrecy about government policy, though, seems to me a very different thing. The whole point of democracy is to make government accountable to the public. How can the public hold government accountable if it doesn’t know what the government’s policies are? How can the public lobby Congress to amend the Patriot Act if it has no idea how the government has interpreted it? This is why I think that you have it backward when you say that “objections to the secrecy of the N.S.A. program are thus really objections to our political system itself.” It’s objections to transparency about the N.S.A. program that have this character. The argument that the government shouldn’t be required to tell the public what its policies are is an argument that we shouldn’t have a democracy.

2. NSA activities threaten our democratic system of government

Jameer Jaffer, Deputy Legal Director, ACLU Foundation and Laura W. Murphy, Director, Washington Legislative Office, ACLU, Testimony before the House Judiciary Committee, 7—17—13, <http://judiciary.house.gov/hearings/113th/07172013/Jaffer%2007172913.pdf>, accessed 10-2-13.

To say that the NSA’s activities present a grave danger to American democracy is no overstatement. Thirty-seven years ago, after conducting a comprehensive investigation into the intelligence abuses of the previous decades, the Church Committee warned that inadequate regulations on government surveillance —threaten[ed] to undermine our democratic society and fundamentally alter its nature.□ This warning should have even more resonance today, because in recent decades the NSA’s resources have grown, statutory and constitutional limitations have been steadily eroded, and the technology of surveillance has become exponentially more powerful. Because the problem Congress confronts today has many roots, there is no single solution to it. It is crucial, however, that Congress take certain steps immediately. It should amend relevant provisions of FISA to prohibit suspicionless, —dragnet□ monitoring or tracking of Americans’ communications. It should require the publication of past and future FISC opinions insofar as they evaluate the meaning, scope, or constitutionality of the foreign-intelligence laws. It should ensure that the public has access to basic information, including statistical information, about the government’s use of new surveillance authorities. It should also hold additional hearings to consider further amendments to FISA—including amendments to make FISC proceedings more transparent.

3. The NSA program is a massive threat to core democratic principles

John Prados, senior fellow, National Security Archive, “Demystifying the NSA Surveillance Program,” HISTORY NEWS NETWORK, 7—15—13, <http://hnn.us/article/152605>, accessed 10-13-13.

A key purpose of law is to prevent the state from trampling the rights of citizens. Here the state has the capability to spy and the citizen has no protection. That Big Brother is watching does not make it right—or legal. The assumption that government will eavesdrop anyway is simply an excuse to avoid the debate which has become so crucial. The fact is that the Fourth Amendment to the Constitution ensures the privacy of the individual in person, property, and effects. The cellphone/notebook/laptop/pc and their contents are personal effects. The surveillance program which targets externals and leads to the surveillance of effects is a plain violation of the Constitution no matter what the excuse. The existence of case law that holds a person has no reasonable expectation of privacy in communications externals—or as quaintly phrased in the Patriot Act, “business records”—merely reflects the history that relevant cases were decided before eavesdropping techniques became as sophisticated as they now are. Individuals cannot even be recognized as standing before the courts to bring suit against these practices, and Government is the only party in actions at the FISC, whose proceedings and decisions are secret. Scarier still, the accumulated NSA database and more intrusive “take” will be used as tools of investigations aimed at ordinary people. The NSA database amounts to a buzz saw hanging over the heads of citizens. This entire framework is a violation of democratic principles. It needs to become part of the debate.

Surveillance Undesirable: Democracy [cont'd]

4. Domestic spying is antithetical to basic democratic principles

Zach Beauchamp, “A Guide to Thinking about NSA Surveillance and Democracy,” THINK PROGRESS, 8—6—13, <http://thinkprogress.org/security/2013/08/06/2423191/surveillance-democracy-nsa/>, accessed 10-12-13.

The issue’s actually more basic that Rosen makes it to be. Spying itself is intrinsically at odds with democratic governance and yet simultaneously something virtually all of us believe the state should be doing, at least to a certain degree. Understanding how to square that theoretical circle clarifies how we should think about the relationship between democracy and the NSA. Democracies, like plants, thrive on sunlight. The heart of a democracy, the idea of government by the consent of the governed, requires that the governed know enough about how they are being governed in order to give real consent. If the government wouldn’t tell me, say, what it was doing with the economy, it’d be hard to argue that I was consenting in any real sense to the economic policies of the current government. Spying is by its very nature antithetical to this basic democratic principle. The CIA, NSA, DIA, and all the other sneaky government organizations whose acronym ends in “A” need to do their work in secret for it to be effective at all. An operation to, say, sabotage Iran’s nuclear program with a computer virus is not the sort of thing that can be announced publicly before launch. So long as we think that some kind of international spying and covert operations is critical to national security (which, even if the specific Iran example isn’t, it in principle almost certainly is), then it seems like we’re consigned to a future in which a significant part of the government is tasked with doing things that can’t in principle be democratically authorized by American citizens.

5. NSA surveillance is anti-democratic because of a lack of meaningful oversight

So what does this theory of spying and democracy tell us about the NSA and Snowden? For one thing, that the problem isn’t, as Rosen suggests, an intrinsic conflict between “electronic surveillance” and “state maneuvering.” Electronic surveillance is merely a subset of broader covert operations; so long as you think covert operations are at all democratically legitimate, then there’s nothing unique about the NSA’s work, or the CIA’s, or so on. In principle, they all raise the same basic question, meaning that focusing on “electronic surveillance” in general is a red herring. The real issue in the NSA case, instead, is oversight. Rosen cites several persuasive reports (including this very good Adam Serwer rundown) suggesting that neither Congress nor the Foreign Intelligence Surveillance Act (FISA) courts were providing meaningful internal checks on the NSA programs that the President had decided couldn’t be disclosed publicly. This means that a basic link in the democratic accountability chain is broken, calling any claim the NSA surveillance regime had on democratic legitimacy into serious question. The most pressing question about NSA reform, from a democratic point of view, is what institutional mechanisms to improve public transparency and internal oversight could be created to limit future abuses. Debating the particular programs in question in this case, while important, risks missing the democratic forest for particular trees.

Surveillance Undesirable: Economic Effects

1. The surveillance programs threaten the competitiveness of U.S. tech companies

Richard Stiennon, “NSA Surveillance Threatens US Competitiveness,” FORBES, 6—7—13, www.forbes.com/sites/richardstiennon/2013/06/07/nsa-surveillance-threatens-us-competitiveness/, accessed 10-13-13.

The vast foreign and domestic spying by the NSA revealed this week threatens the global competitiveness of US tech companies. We are told we live in a digital world and the future is bright for tech startups as costs of launching new products and services plummet and global markets open up to the smallest vendor. Yet, there is a world wide perception that any data that is stored or even routed through the United States is sucked into cavernous NSA data centers for analysis and cataloging. That perception was solidified in 2006 when former AT&T technician Mark Klein blew the whistle on the fiber tap that ATT had provided to the NSA in some of its data centers. Those perceptions have had real consequences for US tech firms seeking to offer global services. Email archiving services such as ProofPoint could not sell to even Canadian customers without building local infrastructure. Even establishing separate data centers in Canada and Europe is not enough to assure customers that their data would forever stay out of the grasp of US intelligence services. One of the fastest growing segments of the tech industry is cloud services, with Salesforce.com one of the leading examples. Box.net, and other cloud storage solutions, are burgeoning. Cloud infrastructure providers like Amazon, Microsoft, and Rackspace are investing billions to serve markets that should be global but will be barred from most countries thanks to the complete abandonment of trust caused by NSA/FBI spying.

2. Dragnet surveillance is only going to damage U.S. business interests

James Fallows, “Why NSA Surveillance Will Be More Damaging than You Think,” THE ATLANTIC, 7—30—13, www.theatlantic.com/technology/archive/2013/07/why-nsa-surveillance-will-be-more-damaging-than-you-think/278181/, accessed 10-4-13.

In short: because of what the U.S. government assumed it could do with information it had the technological ability to intercept, American companies and American interests are sure to suffer in their efforts to shape and benefit from the Internet's continued growth. American companies, because no foreigners will believe these firms can guarantee security from U.S. government surveillance; American interests, because the United States has gravely compromised its plausibility as world-wide administrator of the Internet's standards and advocate for its open, above-politics goals. Why were U.S. authorities in a position to get at so much of the world's digital data in the first place? Because so many of the world's customers have trusted* U.S.-based firms like Google, Yahoo, Apple, Amazon, Facebook, etc with their data; and because so many of the world's nations have tolerated an info-infrastructure in which an outsized share of data flows at some point through U.S. systems. Those are the conditions of trust and toleration that likely will change. The problem for the companies, it's worth emphasizing, is not that they were so unduly eager to cooperate with U.S. government surveillance. Many seem to have done what they could to resist. The problem is what the U.S. government -- first under Bush and Cheney, now under Obama and Biden -- asked them to do. As long as they operate in U.S. territory and under U.S. laws, companies like Google or Facebook had no choice but to comply. But people around the world who have a choice about where to store their data, may understandably choose to avoid leaving it with companies subject to the way America now defines its security interests.

Surveillance Undesirable: Economic Effects [cont'd]

3. The surveillance programs' revelation was inevitable, and will compromise trust in U.S. businesses

James Fallows, "Why NSA Surveillance Will Be More Damaging than You Think," THE ATLANTIC, 7—30—13, www.theatlantic.com/technology/archive/2013/07/why-nsa-surveillance-will-be-more-damaging-than-you-think/278181/, accessed 10-4-13.

Here's Naughton's version of the implications: The first is that the days of the internet as a truly global network are numbered. It was always a possibility that the system would eventually be Balkanised, ie divided into a number of geographical or jurisdiction-determined subnets as societies such as China, Russia, Iran and other Islamic states decided that they needed to control how their citizens communicated. Now, Balkanisation is a certainty.... Second, the issue of internet governance is about to become very contentious. Given what we now know about how the US and its satraps have been abusing their privileged position in the global infrastructure, the idea that the western powers can be allowed to continue to control it has become untenable.... Nothing, but nothing, that is stored in their [ie, US-based companies] "cloud" services can be guaranteed to be safe from surveillance or from illicit downloading by employees of the consultancies employed by the NSA. The real threat from terrorism has never been the damage it does directly, even through attacks as horrific as those on 9/11. The more serious threat comes from the over-reaction, the collective insanity or the simple loss of perspective, that an attack evokes. Our government's ambition to do everything possible to keep us "safe" has put us at jeopardy in other ways. One more note: it is also worth emphasizing that this damage was not done by Edward Snowden, except in an incidental and instrumental sense. The damage comes from the policies themselves, just as the lasting damage from Abu Ghraib came not from the leaked photos but from the abuse they portrayed. What governments do eventually becomes known. Eventual disclosure is likely when a program involves even a handful of people. (Latest case in point: Seal Team Six.) It is certain when an effort stretches over many years, entails contracts worth billions of dollars, and requires the efforts of tens of thousands of people -- any one of whom, as we've seen from Snowden, may at any point decide to tell what he knows. In launching such an effort, a government must assume as a given that what it is doing will become known, and then calculate whether it will still seem "worthwhile" when it does. Based on what we've seen so far, Prism would have failed that test.

Surveillance Undesirable: Economic Effects [cont'd]

4. NSA surveillance threatens business—covers economic activities, threatens trade secrets

Michael German, Senior Policy Council, ACLU Washington Legislative Office, "America, NSA Surveillance Is Bad for Business," Blog of Rights, American Civil Liberties Union, 8—13—13, www.aclu.org/blog/national-security-technology-and-liberty/america-nsa-surveillance-bad-business, accessed 10-8-13.

The New York Times last week provided new information that clarified how a key, yet unnamed, National Security Agency surveillance program designed to "target" foreigners' Internet communications actually worked, namely by secretly snatching and sifting virtually all Americans' international communications. This ubiquitous government surveillance harms more than just our personal privacy, and American businesses need to pay particular attention. Within the piece, a key point was buried in a discussion about the program's ineffectiveness at finding terrorists. An unnamed government official explained "[t]he surveillance was used for other types of foreign intelligence collection, not just terrorism." "Foreign intelligence" is defined broadly in the statute, to include any information relating to U.S. "foreign affairs," which the government interprets to include trade, travel, currency transactions, and international business matters. We believe this puts American companies in the crosshairs of these collection programs. Here is a letter I wrote several years ago in preparation for a meeting with business groups when Congress passed the first version of the bill that authorized this type of broad surveillance. Unfortunately, our concerns haven't changed much. (The following has been slightly edited to account for a 2008 update to the law): On August 4, 2007 Congress changed the nature of the relationship American citizens have with their government. The Fourth Amendment to the U.S. Constitution guaranteed the right of the people "to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures," or put more simply, the right to be left alone absent probable cause and a warrant issued by a neutral magistrate. But now our government can seize the private international communications of all Americans and search them for "foreign intelligence information" without any suspicion that anyone has done anything wrong. Congress accomplished this ignoble task by altering the definition of "electronic surveillance" so as to exclude any government eavesdropping that is directed at an entity "reasonably believed" to be outside the United States from coverage under the protections of the Foreign Intelligence Surveillance Act. Now when an American is calling his aunt in Italy, or e-mailing his business associate in Canada, or engaging in an Internet chat where one of the parties could be overseas [snip] the government can listen in without any court oversight. This is a fundamental change that has serious ramifications for all Americans, but especially for American companies that do business in the global economy. Congress gave the government this eavesdropping authority not to listen to terrorists, but rather to collect "foreign intelligence," which is loosely defined in FISA to mean any information that "relates to" the conduct of U.S. foreign affairs. Make no mistake, this means business. The rapid expansion of e-commerce now allows small mom-and-pop companies in the heartland of America to sell their products in foreign markets. Because of the bill Congress passed your international business transactions can now be monitored by the government. Globalization and free trade agreements have made it easier for U.S. companies to have an international workforce. Now your communications with those foreign employees can be monitored by the government. The "flattening" of the world opened new opportunities for Americans to invest in growing world markets and to provide charitable gifts to areas in desperate need. Now your international investments and philanthropy can be monitored by the government- not because you are suspected of doing anything wrong, but simply because the government wants foreign intelligence information. Congress could have easily restricted this new authority to investigations of suspected terrorists, but it did not. Any businessperson can easily see the ramifications of such unwarranted surveillance. How are trade secrets going to be protected? Are negotiations regarding government contracts being conducted in good faith, or are they being compromised by intercepted communications? How are confidential relationships- employer/employee; attorney/client; journalist/source; doctor/patient; priest/penitent; husband/wife- going to be protected? How are these captured communications going to be used against you and your business? The answer is nobody knows because it's all being conducted behind a massive cloak of secrecy. American companies have much to lose from these government surveillance programs. When foreign businesses and customers lose confidence that American companies can maintain confidentiality in their business dealings and financial transactions, they will likely look for other, more secure partners. According to a report released last week by The Information Technology & Innovation Foundation, NSA surveillance could cost the U.S. cloud computing industry anywhere from \$22 to \$35 billion over the next three years if "foreign customers decide the risks of storing data with a U.S. company outweigh the benefits."

Surveillance Undesirable: Economic Effects [cont'd]

5. The spying is crushing business opportunities for U.S. tech companies

Richard Stiennon, “NSA Surveillance Threatens US Competitiveness,” FORBES, 6—7—13, www.forbes.com/sites/richardstiennon/2013/06/07/nsa-surveillance-threatens-us-competitiveness/, accessed 10-13-13. Trust is the very foundation of all commerce. Once lost it is almost impossible to regain. This week’s revelations that the NSA has blanket data harvesting arrangements with Verizon, ATT, Sprint-Nextel, Google, Microsoft, Apple, Skype, Yahoo, FaceBook and even credit card processors, will have immediate repercussions. Non-US customers of any US business will immediately evaluate their exposure to these new risks and look for alternatives. European, Canadian, and Australian tech companies will profit from this. Competitors in those regions will offer alternatives that will also draw US customers away from the compromised US services. While the FBI and NSA leverage the dramatic intelligence opportunities of a digital world, their Orwellian actions are crushing opportunity for tech giants and startups in the United States.

6. Surveillance threatens U.S. business—loss of trust

Susan Waterman, “Wyden: NSA Eavesdropping Is Hurting U.S. Economy,” WASHINGTON TIMES, 10—9—13, www.washingtontimes.com/news/2013/oct/9/wyden-nsa-eavesdropping-hurting-us-economy/, accessed 10-10-13. Revelations about the National Security Agency’s monitoring of online communications have damaged the U.S. economy so badly that Americans should “be in the street with pitchforks,” according to a senator leading the effort to reform federal surveillance laws. Sen. Ron Wyden, Oregon Democrat, told a day-long conference at the Cato Institute, a libertarian think tank, that U.S. companies trying to do business in the global technology and communications market are hurting because of the revelations that American Internet giants like Microsoft, Google and Facebook have been under court order to cooperate with the NSA to monitor Web traffic. “If a foreign enemy was doing this much damage to the economy, people would be in the streets with pitchforks,” Mr. Wyden said. A recent report from the Information Technology and Innovation Foundation, a nonprofit, public policy think tank, estimated that the U.S. cloud computing industry alone stands to lose up to \$35 billion over the next three years as a result of the revelations — and its impact on the reputation and customer relations of U.S. firms. American firms weren’t just given that reputation, “they won it over the years with good customer practices” only to see it swept away by “this overly broad surveillance,” Mr. Wyden said. Analysts say that a particular problem is that many overseas customers now understand that the U.S. Constitution offers them no protection from NSA eavesdropping.

Surveillance Undesirable: International Backlash—Europe

1. The surveillance programs are spurring a massive backlash from our European allies, threatening cooperation

Ryan Gallagher, fellow, New America Foundation, "Obama Administration's Indifference on NSA Surveillance Fuels Fury in Europe," SLATE, 7—2—13, www.slate.com/blogs/future_tense/2013/07/02/obama_administration_s_indifference_on_nsa_surveillance_fuels_fury_in_europe.html, accessed 10-11-13.

For almost a month, revelations about the National Security Agency's surveillance programs have made headlines across the world. But the international legal and political backlash is only just beginning. In June, details about the NSA's efforts to spy on foreigners' communications sparked outrage in Europe, prompting calls for renewed efforts to strengthen data protections regulations. Now, the rhetoric is being replaced with action. Following the exposure of the NSA's Internet snooping system PRISM, the vice president of the European Commission, the EU's executive body, squared up to Attorney General Eric Holder over the scope of the program. Further information published by the Guardian on Sunday revealed that the NSA is not only monitoring foreigners for intelligence-gathering and counter-terrorism purposes, but it is also bugging diplomatic missions used by EU officials. This has prompted France to threaten to halt European trade talks unless the United States "immediately" stops its surveillance of allies, potentially jeopardizing a free-trade agreement worth billions of dollars every year. President Obama and Secretary of State John Kerry have tried to play down the spying, insisting that bugging allies is normal behavior conducted by all intelligence agencies. But the administration's dismissive remarks appear to have only provoked further anger among some European leaders, who seem genuinely shocked and aghast at the scope of the NSA's activities. Martin Schulz, the president of the European Parliament, described the surveillance as "comparable to measures taken in the past by the KGB, by the secret service of the Soviet Union."

2. The backlash from European allies threatens relations

Josh Levs and Catherine E. Schoichet, "Europe Furious, 'Shocked' by Report of U.S. Spying," CNN, 7—1—13, <http://www.cnn.com/2013/06/30/world/europe/eu-nsa/index.html>, accessed 10-11-13.

European officials reacted with fury Sunday to a report that the U.S. National Security Agency spied on EU offices. The European Union warned that if the report is accurate, it will have tremendous repercussions. "I am deeply worried and shocked about the allegations," European Parliament President Martin Schulz said in a statement. "If the allegations prove to be true, it would be an extremely serious matter which will have a severe impact on EU-US relations. On behalf of the European Parliament, I demand full clarification and require further information speedily from the U.S. authorities with regard to these allegations." Bush on Snowden: He damaged the country Still looking for Edward Snowden Deal offered for Snowden's return Obama covers his bases on Snowden German Justice Minister Sabine Leutheusser-Schnarrenberger "said if the accusations were true, it was reminiscent of the Cold War," ministry spokesman Anders Mertzlufft said, adding that the minister "has asked for an immediate explanation from the United States." French Foreign Minister Laurent Fabius called for a swift explanation from American authorities. "These acts, if they are confirmed, would be absolutely unacceptable," he said in a statement. The outrage from European officials over the weekend was the latest fallout since Edward Snowden, a former National Security Agency computer contractor, started spilling details of U.S. surveillance programs to reporters earlier this month.

3. The programs threaten vital cooperation from allies

John Prados, senior fellow, National Security Archive, "Demystifying the NSA Surveillance Program," HISTORY NEWS NETWORK, 7—15—13, <http://hnn.us/article/152605>, accessed 10-13-13.

Allies the NSA monitored are talking out of both sides of their mouths because allies spy on each other all the time. This argument is one more instance of obfuscation in the NSA scandal. Nations, including allies, do spy on each other all the time. No question. But the contention here is misleading in two ways. First, allies hope to be handled more delicately than enemies. The NSA surveillance, by aiming at communications mechanisms, automatically focuses on those countries with the most developed communications infrastructures, which include America's closest allies and many of our best friends. This is especially pernicious in that some of these same allies are our closest collaborators in the war on terror. Their cooperation is essential. Anything that weakens those ties is a negative, not a positive value. Second—and equally, if not more important—spying on allies is traditionally done in service of national objectives. A present flap over whether the NSA had the goal of penetrating European strategies for trade talks currently in progress is an example of old style spying. But the NSA's eavesdropping, which aims at individuals and uses targeting priorities that focus on foreign nationals, goes far beyond the old style spying. Moreover, so far as we now know, the strictures against the NSA reading content, as opposed to vacuuming metadata, do not apply to foreign nationals. Millions of citizens in friendly lands are now personal quarry of NSA eavesdropping. The outpouring of protest in Germany, in France, in Latin America against the U.S. surveillance has much to do with this sense of personal violation.

Surveillance Undesirable: International Backlash—Europe [cont'd]

4. The surveillance program has prompted a major backlash in Germany and among other allies

Ryan Gallagher, fellow, New America Foundation, "Obama Administration's Indifference on NSA Surveillance Fuels Fury in Europe," SLATE, 7—2—13, www.slate.com/blogs/future_tense/2013/07/02/obama_administration_s_indifference_on_nsa_surveillance_fuels_fury_in_europe.html, accessed 10-11-13.

In Germany, a country with a touchy relationship with privacy due to the brutal legacy of East Germany's Stasi secret police, revelations about the NSA explicitly targeting Germans' communications for mass surveillance have incensed both the public and political class alike. A spokesman for German Chancellor Angela Merkel said that "bugging friends is unacceptable" and added that "we are no longer in the cold war." German newspaper Der Spiegel reported Sunday that federal prosecutors in the country are investigating the NSA's spying and that criminal complaints will likely be issued in relation to the scandal. Elsewhere, government officials in Luxemburg, Austria, Turkey, and Japan have demanded answers from the Obama administration about the NSA's spying efforts. And U.N. Secretary General Ban Ki-moon said Monday when asked about the U.S. bugging diplomatic missions that international law means "diplomatic activities should be protected." Indeed, the 1961 Vienna convention on diplomatic relations specifically states that "the official correspondence of the mission shall be inviolable." But that does not appear to have stopped the NSA, which reportedly deemed 38 embassies and missions "targets" for covert communications surveillance. The classified documents leaked by NSA contractor Edward Snowden continue to illustrate how the agency has spread its surveillance tentacles around the world. It is possible, however, that the forced transparency Snowden has brought about with his leaks may lead to a culture-shift in the NSA's activities. Public opinion on the NSA's spying is divided in the United States. But international legal cases and mushrooming diplomatic fallouts in Europe and elsewhere could make the difference—reining in aggressive surveillance programs that appear to have spiralled to alarming proportions under cover of total secrecy.

5. The program has infuriated our German allies

Jason Ditz, "NSA Surveillance Threatens US Relations with Germany," ANTIWAR, 8—25—13, <http://news.antiwar.com/2013/08/25/nsa-surveillance-threatens-us-relations-with-germany/>, accessed 10-11-13.

Most of the focus on NSA surveillance has been the domestic fallout from the Obama Administration spying on ordinary Americans and then lying repeatedly about it. The international fallout is significant, however, with key US allies like Germany and Brazil taking the revelation of systematically being targeted poorly. Germany is particularly outraged by the NSA spying, with the nation's substantial privacy laws aimed at preventing the sort of surveillance state the US is now imposing on them, and German officials running for cover as the revelations loom large in the September elections. Germany has been a major target for the NSA, and continues to be so because of the nation's status as a major economic power and its influence in the European Union. The fear of corporate espionage conducted by the US government masquerading as "anti-terror" operations is huge, as is the threat to ordinary peoples' privacy. The German government is now focusing on getting the US to agree to a new treaty promising not to spy on one another. Since German is less the spy-er than the spy-ee, it's going to be a tough battle to convince the US on it, and officials are going to have to leverage other pacts.

6. The program threatens U.S. interests—international backlash to spying

Lauren McCauley, "Global Backlash After Leaks Reveal Hypocrisy of US Spying," COMMON DREAMS, 6—27—13, <https://www.commondreams.org/headline/2013/06/27-7>, accessed 10-11-13.

Three weeks since news broke that the National Security Administration is conducting a massive international surveillance operation, the US corporate media is still largely consumed by the witch-hunt for NSA whistleblower Edward Snowden and smear campaigns against Snowden and Guardian journalist Glenn Greenwald, to whom Snowden revealed the leaked documents. However, the international community has reacted to the disclosures with alarm. Revelations that the NSA has been tapping the phone and internet communications of foreign individuals and governments has spurred world leaders to denounce the global superpower as a 'hypocrite' and, in a number of instances, offer asylum or assistance to Snowden. "The Prism-gate affair is itself just like a prism that reveals the true face and hypocritical conduct regarding Internet security of the country concerned," said Chinese Ministry of National Defense Spokesperson, Colonel Yang Yujun. Sir Tim Berners-Lee, one of the five individuals who is credited as being a 'father of the internet' agreed telling the London Times newspaper that the 'insidious' spying by the United States was hypocritical in light of the US government's frequent 'policing' of other states. "In the Middle East, people have been given access to the Internet but they have been snooped on and then they have been jailed," he said. "It can be easy for people in the West to say 'oh, those nasty governments should not be allowed access to spy.' But it's clear that developed nations are seriously spying on the Internet." The dramatic international backlash is a clear indication of the importance and severity of the leaked information and, in the interest of insuring that these revelations are not eclipsed by more distracting headlines, below is a summary of what we know so far about the NSA's spy program.

Surveillance Undesirable: International Backlash—Latin America

1. The program has caused a major backlash from Brazil

Catherine E. Shoichet, "As Brazil's Uproar over NSA Grows, U.S. Vows to Work through Tensions," CNN, 9—12—13, <http://www.cnn.com/2013/09/11/world/americas/brazil-nsa/index.html>, accessed 10-11-13.

As the furor mounts in Brazil over reports that the United States spied on President Dilma Rousseff and her advisers, the South American country's foreign minister was in Washington on Wednesday. U.S. National Security Advisor Susan Rice told Brazilian Foreign Minister Luiz Alberto Figueiredo that the United States is committed to working with Brazil to address its concerns, the White House said in a statement. But in Brazil, debate over media reports about alleged National Security Agency spying showed no signs of cooling. Brazilian lawmakers say they plan to send a commission to Russia to speak directly with former NSA contractor Edward Snowden, who reportedly leaked documents cited in Brazilian media reports about the alleged espionage operations. Reports from Globo TV citing Glenn Greenwald, a Brazil-based journalist who obtained documents from Snowden, claim that Rousseff and the state oil company Petrobras were among the targets of the NSA. Why are Brazil, Mexico angry with NSA? NSA surveillance revelations Open Mic: Russians on Edward Snowden CNN has not independently verified the reports, which drew sharp condemnation from Brazilian officials this month. A foreign relations committee in Brazil's Chamber of Deputies on Wednesday approved a trip for lawmakers to travel to Moscow and interview Snowden over the matter, state-run Agencia Brasil reported. Lawmaker Ivan Valente said authorities wanted more information, not just what had been leaked to the media. "The leaked information is an issue of national sovereignty," he said, according to Agencia Brasil. "First, Brazilian citizens were spied on. Then companies, the president of the republic, ministers and now Petrobras." Earlier this month, Brazil summoned the U.S. ambassador over the reports. And Rousseff has threatened to cancel her scheduled state visit to Washington in October.

2. Backlash is widespread—Mexico, Brazil Europe

Catherine E. Shoichet, "As Brazil's Uproar over NSA Grows, U.S. Vows to Work through Tensions," CNN, 9—12—13, <http://www.cnn.com/2013/09/11/world/americas/brazil-nsa/index.html>, accessed 10-11-13.

Reports from Brazil's Globo TV over the alleged espionage have also drawn Mexico's ire, with allegations that the NSA spied on Mexican President Enrique Peña Nieto. U.S. President Barack Obama said he promised to look into the allegations when he spoke with Peña Nieto and Rousseff at last week's G-20 summit in St. Petersburg. "What I assured President Rousseff and President Peña Nieto is...that I take these allegations very seriously," Obama told reporters. "I understand their concerns; I understand the concerns of the Mexican and Brazilian people, and that we will work with their teams to resolve what is a source of tension." The diplomatic tensions with Brazil and Mexico are the latest international fallout over documents leaked by Snowden, who faces espionage charges in the United States and is now living in Russia after authorities there granted him temporary asylum. Reports of U.S. espionage also roiled European officials over the summer after Germany's Der Spiegel and Britain's The Guardian published stories alleging that the NSA had targeted European government offices.

3. The program has caused a backlash throughout Latin America

Anthony Boadle, "NSA Surveillance: Latin American Countries Demand Explanation of U.S. Spying Programs," REUTERS, 7—11—13, www.huffingtonpost.com/2013/07/11/nsa-surveillance-latin-american-countries_n_3579080.html, accessed 10-11-13.

Irate Latin American nations are demanding explanations from the United States about new allegations that it spied on both allies and foes in the region with secret surveillance programs. A leading Brazilian newspaper reported on Tuesday that the U.S. National Security Agency targeted most Latin American countries with spying programs that monitored Internet traffic, especially in Colombia, Venezuela, Brazil and Mexico. Citing documents leaked by Edward Snowden, the fugitive former U.S. intelligence contractor, O Globo newspaper said the NSA programs went beyond military affairs to what it termed "commercial secrets," including oil and energy resources. Regional leaders called for a tough response to the alleged espionage that O Globo said included a satellite monitoring stations based in Brazil's capital. "A shiver ran down my back when I learned that they are spying on all of us," Argentine President Cristina Fernandez said in a speech on Tuesday. She called on the Mercosur bloc of South American nations, due to meet on Friday, to issue a strong statement and demand explanations from Washington. "More than revelations, these are confirmations of what we thought was happening," she said. Peruvian President Ollanta Humala, who has emerged as a close U.S. ally, said the reported spying was worrisome. "We are against these kinds of espionage activities," he said in a televised interview. "It would be good for (Peru's) Congress to look with concern at privacy issues related to personal information." Brazil's government said it set up a task force of its defense, communications, justice and foreign affairs ministries to investigate the alleged espionage and establish whether the privacy of Brazilian citizens had been violated.

Surveillance Undesirable: International Law

1. The NSA programs stand in violation of the International Covenant on Civil and Political Rights

G. Alex Sinha, fellow, Human Rights Watch, “NSA Surveillance Since 9/11 and the Human Right to Privacy,” *LOYOLA LAW REVIEW*, 8—31—13, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2327806, accessed 10-12-13.

Both the Human Rights Committee and Manfred Nowak argue that Article 17 permits interference with the right to privacy only when it is lawful, non-arbitrary, and proportionate to the pursuit a legitimate aim. The preceding analysis highlights a number of ways in which the NSA program seems both unlawful and arbitrary, fatal flaws under the dominant interpretation of Article 17. Even if the United States were to take the position—in good faith—that the NSA program is essential for national security, the standard analysis would seem to suggest that the program needs substantial revisions to bring it into line with the terms of the ICCPR. We have already foreclosed the possibility that national security could justify unlawful and arbitrary interference with the right to privacy; that reading is implausible on its face because of its implications, not to mention the fact that it is in tension with the major interpretations of the ICCPR and the European Convention. Suppose, however, that the United States were to argue that national security interests are so important that they render the program lawful and non-arbitrary. Perhaps the program is lawful because by definition it supports the pursuit of an important (even overriding) goal; and the program is not arbitrary because it is animated by that goal. For this position to stand, we would need to reject the view that lawfulness and arbitrariness contain independent content (as elucidated by the Committee and various commentators above), such that the reason for interference is not itself proof of lawfulness or non-arbitrariness. This would be an odd result, requiring an unusual interpretation of the terms “lawful” and “arbitrary.” An unreasonable search in domestic law is not automatically rendered reasonable because it purportedly served an important purpose—even if that purpose is relevant in other ways. Moreover, there remains the matter of the requirement that policies that do interfere with the right to privacy must be proportionate to securing a legitimate aim. Even if the purpose somehow made the policies legal and non-arbitrary, it is not at all clear that the NSA program is proportionate to its goal—especially if the intrusions into privacy are as severe as multiple reports have suggested, and if the data points collected are so numerous that the government lacks the ability even to sort through them effectively. In the end, however, entertaining this argument is more a matter of completeness than a matter of serious legal analysis. All along, we have made charitable assumptions toward the position of the United States, specifically to ensure a conservative and compelling series of conclusions. But there are only so many times that we can take the position favorable the United States and keep the results plausible, and by now we seem to have exhausted that supply. The more promising indicator for the United States is the deference of the ECtHR in cases where state parties assert national security as the justification for their interference with the right to privacy. Recall that the ECtHR places substantial weight on the existence of “formal legality and procedural guarantees,” as well as access to remedies. If those conditions are met, then the ECtHR is likely to defer in the face of interference with the right to privacy (under Article 8 of the European Convention). Even here, however, the United States would struggle. For much of its life, the NSA program lacked formal legality, and even now it has weak procedural guarantees. Further, in light of *Clapper*, access to remedies is severely restricted. Perhaps it would be possible for the United States to modify the NSA program in a way that allowed it to retain its breadth while also complying with the sort of criteria valued by the ECtHR, but until and unless that were to happen, a favorable verdict by analogy for the legality of the NSA program under the ICCPR is unlikely. In sum, it is obviously difficult to reach conclusive opinions about the legality of the NSA program (or its various constituent parts) under the ICCPR in part because some of our analysis is built on credible but disputed or unsubstantiated reporting on the program itself. At the very least, we need additional, concrete information about how the government executes the program. Further, the arguments on either side are relatively complicated, and can develop in a range of different ways. But at a minimum, even on conservative assumptions about the nature of the program and the scope of the ICCPR, we face the legitimate and frightening prospect that the United States is systematically and massively violating the human right to privacy.

Surveillance Undesirable: International Law [cont'd]

2. The U.S. needs to uphold its human rights obligations

G. Alex Sinha, fellow, Human Rights Watch, “NSA Surveillance Since 9/11 and the Human Right to Privacy,” *LOYOLA LAW REVIEW*, 8—31—13, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2327806, accessed 10-12-13.

Nevertheless, the question is an important one. Having chosen to bind itself to the terms of the ICCPR, gaining whatever public relations and political benefits such a choice entails, the United States may not simply disregard the attendant legal obligations. If it turns out that the United States is violating the terms of Article 17, then only a series of very specific conditions could allow the United States to escape the conclusion that it is in violation of its human rights obligations. As it happens, those conditions—relating to derogation under the terms of the ICCPR, or to reservations, understandings and declarations (“RUDs”) attached by the United States to the relevant article of the ICCPR—do not obtain in this case. Thus, in essence, if the NSA program violates the protections laid out in the ICCPR, then the United States is also violating its human rights obligations. This conclusion, if warranted, would be significant for a number of reasons. First and foremost, human rights treaties and covenants are designed to prevent human rights violations—and with good reason. Accordingly, as a normative matter, we should not simply abide human rights violations without any public debate in those terms, and without an explicit (and legitimate) justification from the violator. The United States has argued that the program is legal under domestic law—though many commentators and some federal judges have disagreed. To the best of my knowledge, however, the government has not explained why the program is legal under the ICCPR. Moreover, for a state that has historically emphasized the importance of civil and political rights (above social and economic rights), it would be especially problematic for the United States to violate the right to privacy, which is a quintessential civil and political right. While the United States has pushed the envelope aggressively even on other civil and political rights—in particular, for example, due process rights for those accused or suspected of terrorism—the NSA program implicates the rights of American citizens located within the United States’ own borders. Even if no moral reasons obviously privilege American citizens living at home, we shall see that there is a formal, legal distinction held out by the United States that would seem to make its comportment vis-à-vis people living within its borders all the more important. Finally, if it is illegal, given the apparent scope of the NSA program, the number of violations of the human right to privacy could easily climb into the millions, billions, or even trillions. The extensive and systematic nature of the program could thus compel the conclusion that the United States is violating the human right to privacy within its borders on a truly colossal scale.

3. The surveillance programs violate international human rights law

G. Alex Sinha, fellow, Human Rights Watch, “NSA Surveillance Since 9/11 and the Human Right to Privacy,” *LOYOLA LAW REVIEW*, 8—31—13, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2327806, accessed 10-12-13.

Since shortly after 9/11, the National Security Agency (“NSA”) has been collecting massive amounts of data about American citizens and permanent residents, ostensibly with the aim of preempting future terrorist attacks. While the NSA’s program has invited substantial scholarly attention, specifically surrounding its compliance with the United States Constitution and various domestic statutes, the academic debate about its merits entirely omits one crucial fact: the United States is also legally obliged to protect a human right to privacy, as codified in Article 17 of the International Covenant on Civil and Political Rights (“ICCPR”). This paper seeks to eliminate the blind spot caused by that omission, illustrating the relevance of human rights for assessing the legality and propriety of NSA surveillance. It argues that even under conservative assumptions about the scope of the NSA program and the coverage of the ICCPR, there is good reason to think that the program violates the covenant.

Surveillance Undesirable: International Law [cont'd]

4. The NSA program violates international law—overcollection

G. Alex Sinha, fellow, Human Rights Watch, “NSA Surveillance Since 9/11 and the Human Right to Privacy,” LOYOLA LAW REVIEW, 8—31—13, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2327806, accessed 10-12-13.

These instances appear problematic for the United States’ obligations under the ICCPR. Even if these violations of domestic law occurred by accident—and only some of them did—they nevertheless occurred in contravention of the operative legal framework and potentially to the detriment of millions of Americans. Moreover, the fact that the NSA broke the law so many times suggests a systemic problem, perhaps a lax approach by the agency toward its international human rights obligations as an arm of the United States Government. Indeed, as noted previously, the rate of inadvertent over-collection incidents appears to have increased over the period of the internal May 2012 audit. Additionally, the Human Rights Committee is crystal clear on what should happen when the government accidentally collects information on individuals improperly: “If [one’s personal data, stored in automatic data] files contain incorrect personal data or have been collected or processed contrary to the provisions of the law, every individual should have the right to request rectification or elimination.” Suffice it to say that the United States has never offered publicly to disclose such information to those who have been wronged by over-collection, nor made clear that it will adjust its databases accordingly by deleting the information that was gathered improperly. (It is worth noting that there is at least one reported instance of the NSA “purging” improperly collected information, which took place in April of 2012, a few months after the agency had satisfied the FISC that it had replaced its unconstitutional search provision.) Indeed, in the wake of the Supreme Court decision in *Clapper*, Americans have no legal recourse to challenge domestic surveillance under the now-operative FAA if they cannot prove that they were harmed; thus, even justified suspicion that one has had his communications or information improperly collected is insufficient to provide standing for a legal remedy.

5. The programs violate international law—arbitrary nature

G. Alex Sinha, fellow, Human Rights Watch, “NSA Surveillance Since 9/11 and the Human Right to Privacy,” LOYOLA LAW REVIEW, 8—31—13, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2327806, accessed 10-12-13.

Aside from the controversial “extra-legal” beginnings of the NSA program, another major point of concern from critics is precisely that it is arbitrary. There are several ways in which the program might trigger concern under the “arbitrariness” prong of Article 17. One relates to the number of times that the government has accidentally or unintentionally gathered more information than it had aimed to gather. Accidental over-collection of data is arbitrary by definition (even in the subset of cases where it is also legal under domestic law) because it is not executed for cause. Such collection would be especially problematic in those cases lacking a legitimate auxiliary justification for collecting the data, but is troubling even otherwise. Moreover, the consistency with which errors at the NSA result in its over-collecting data—thousands of times per year in D.C.-area offices alone—reveals a systemic problem with significant implications for the covenant’s non-arbitrariness requirement. Additionally, recall further the allegations of a former NSA analyst that the agency had gained warrantless access to Americans’ emails through a large database called “Pinwale,” beginning as early as 2005. The analyst claimed that the agency would run searches in the database and accept an incidental yield of Americans’ communications as high as 30%. These claims suggest a protocol that routinely permitted the substantial, unintended over-collection of data in a manner that does not itself register as a problem within the NSA. Such collection would seem to be arbitrary in the sense of lacking cause, and is unlikely to be reported as an “incident” on an internal audit because it falls within the agency’s defined parameters for acceptable rates of error.

Surveillance Undesirable: Privacy—General

1. Current programs raise serious privacy concerns

Jameer Jaffer, fellow, Open Society Foundations, “Secrecy and Freedom,” NEW YORK TIMES, Room for Debate, 6—9—13, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined>, accessed 10-4-13.

The revelations about the National Security Agency’s domestic surveillance activities supply further evidence, if any were needed, that our surveillance laws are too permissive, our privacy safeguards too weak, and our oversight mechanisms utterly dysfunctional. The Guardian revealed on Wednesday that the government has directed Verizon Business Network Services to hand over an array of sensitive information about every domestic and international phone call made by its customers in the United States over a three-month period. The directive, sanctioned by the secretive court that oversees government surveillance in some national security cases, requires Verizon to tell the government who made each call, whom they called, when they made the call, how long the call lasted, and (maybe) where the parties to the call were located. Reportedly, the N.S.A. has been serving all of the major telecommunications companies with similar “metadata” directives for at least seven years. Whatever else might be said about it, the program surely constitutes one of the most ambitious surveillance efforts ever undertaken by a democratic government against its own citizens. As if that weren’t enough, The Guardian and The Washington Post also revealed last week that the N.S.A. has secured direct access to the major Internet companies’ central servers. There seems to be some confusion about precisely what the N.S.A. is doing with that access, but The Washington Post reports that the agency is collecting information about surveillance targets believed (with 51 percent certainty) to be outside the United States and about people one and two degrees removed from these targets. So the N.S.A. might focus initially on, say, a British journalist working at Der Spiegel, collecting all of her e-mail communications as well as all uploaded videos, photos, Web surfing data, social media posts — and then collect the same information about all of the contacts in the journalist’s address book and then about all of the contacts in their address books. On Friday, in an effort to quell a swelling tide of criticism, President Obama observed that these surveillance activities had been blessed by all three branches of government. That observation is alarming, not reassuring. Congress should have more narrowly limited the N.S.A.’s authority to monitor the communications of innocent people. The agency should never have sought the authority to cast an indiscriminate dragnet. The court should never have granted it. The surveillance activities disclosed last week are the result of systemic failure — a failure of all three branches of government — and if we are going to restore some measure of the privacy that the Constitution guarantees, we will need systemic reform.

2. Small intrusions snowball—we need to resist them and work to protect our liberty

Elizabeth Goitein, co-director, Liberty and National Security Program, Brennan Center for Justice, New York University School of Law, “The Danger of American Apathy on NSA Surveillance,” CHRISTIAN SCIENCE MONITOR, 7—31—13, www.csmonitor.com/Commentary/Opinion/2013/0731/The-danger-of-American-apathy-on-NSA-surveillance, accessed 10-13-13.

Serious as they are, these concerns fail to explain fully why Americans should care. After all, this remains a remarkably free country. There are exceptions. Muslim Americans, who are singled out for scrutiny by some law enforcement agencies, have reported harassment by customs officials as well as a chilling of political and religious activity. Outside of these communities, though, few Americans feel any tangible effects from increased surveillance. The vast majority of law-abiding citizens go about their lives without fear of government persecution. And that may be the problem. Free societies tend to take their freedom for granted. But our liberties do not derive from the innate trustworthiness of our elected representatives. They derive from laws and institutions put in place for the preservation of liberty. These laws and institutions, some version of which can be found in all democratic societies, are relatively recent innovations in human history. Before their advent, tyrannies and dictatorships were the norm. Even today, in countries without this framework, people are not free. Since 9/11, the laws and institutions created to ensure Americans’ freedom have been weakened — sometimes incrementally, sometimes significantly — at a rapid pace. This is particularly true for limitations on surveillance, a power that carries tremendous potential for abuse. National Security Letters, a form of administrative subpoena, are now available to collect any information “relevant” to a terrorism investigation, not just information about potential suspects. Customs agents no longer need reasonable suspicion of wrongdoing to search citizens’ laptops at the border. Americans’ international communications are now subject to wiretapping without an individualized court order. The list goes on. In any given instance, the government can make the case that the change is small, or that it is justified by increased security. In some cases, the argument may be persuasive. It is the trend, however, that should concern us. Twelve years after 9/11, as the nation approaches the date for withdrawing troops from Afghanistan, the quiet erosion of Americans’ civil liberties continues.

Surveillance Undesirable: Privacy—General [cont'd]

3. Data mining poses an enormous threat to our privacy and other personal liberties

Danielle Keats Citron and David Gray, University of Maryland School of Law, “Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards,” *HARVARD LAW REVIEW FORUM* v. 126, 2013, p. 264-265.

Congressional panels, journalists, and citizens have been told that fusion centers raise few privacy concerns and that their information gathering is focused and valuable. Contrary to these assurances, critics have argued that fusion centers erode civil liberties without concomitant gains for security. A recent Congressional report backs these concerns, demonstrating that fusion centers have amounted to a waste of resources. Fusion centers cast a wide and indiscriminate net. Data-mining tools analyze a broad array of personal data culled from public- and private-sector databases, the Internet, and public and private video cameras. Fusion centers access specially designed data-broker data-bases containing dossiers on hundreds of millions of individuals, including their Social Security numbers, property records, car rentals, credit reports, postal and shipping records, utility bills, gaming, insurance claims, social network activity, and drug- and food-store records. Some gather biometric data and utilize facial-recognition software. On-the-ground surveillance is collected, analyzed, and shared as well. For example, the San Diego fusion center purchased tiny cameras for law enforcement to attach to their shirt buttons, hats, and water bottles. Through the federal government’s “Information Sharing Environment,” information and intelligence is distributed to public entities, including state, local, and federal agencies, and private owners of “critical infrastructure,” such as transportation, medical, and telecommunications infrastructure.

4. These programs risk the rise of a surveillance state

Danielle Keats Citron and David Gray, University of Maryland School of Law, “Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards,” *HARVARD LAW REVIEW FORUM* v. 126, 2013, p. 269-270.

In assessing the privacy interests threatened by such totalizing surveillance, we have in mind some of the lessons taught by Samuel Warren and Louis Brandeis in their foundational article *The Right to Privacy*. Of course, the surveillance technologies of their era could only record discrete slices of life. Nonetheless, Warren and Brandeis recognized that emerging surveillance capacities threatened individuals’ interests in being “let alone” in their “private life, habits, acts, and relations.” In Warren and Brandeis’s view, the watchful eye of “any other modern device for recording or reproducing scenes or sounds” interfered with the development of a person’s “inviolable personality.” In discussing a husband’s note to his son that he did not dine with his wife — a pedestrian communication by any measure — Warren and Brandeis explained that the privacy interest protected was “not the intellectual act of recording the fact that the husband did not dine with his wife,” but the unwanted observance of the “domestic occurrence” itself. Of course, these are precisely the concerns echoed by Justice Scalia on behalf of the Court in *Kyllo*. The threat posed by contemporary surveillance technologies lies in how much and how often people are watched. Modern technologies allow observers to detect, gather, and aggregate mass quantities of data about mundane daily acts and habits as well as “intellectual” ones. The continuous and indiscriminate surveillance they accomplish is damaging because it violates reasonable expectations of quantitative privacy, by which we mean privacy interests in large aggregations of information that are independent from particular interests in constituent parts of that whole. To be sure, the harms that Richards links to intellectual privacy are very much at stake in recognizing a right to quantitative privacy. But rather than being a function of the kind of information gathered, we think that the true threats to projects of self-development and democratic culture lie in the capacity of new and developing technologies to facilitate a surveillance state.

Surveillance Undesirable: Privacy—Monitoring of Innocents

1. The NSA programs are highly intrusive and surveil people who have done nothing wrong

G. Alex Sinha, fellow, Human Rights Watch, “NSA Surveillance Since 9/11 and the Human Right to Privacy,” *LOYOLA LAW REVIEW*, 8—31—13, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2327806, accessed 10-12-13.

Second, the NSA program also threatens to be arbitrary because of its overwhelming size, and what the size implies about standards of suspicion. The NSA has a reason for wanting to collect as much information as possible, which differentiates massive, deliberate collection from systematic if unintended over-collection; but given the sensitivity of the information sought, merely finding utility in collecting the information is unlikely to save the program from violating the non-arbitrariness restriction. The allegations of David Kris and James Binney are particularly relevant here, but even if we take a skeptical position on their claims, the reporting of the Washington Post that close to 2 billion calls and emails are intercepted every day raises questions about how the collection could fail to be capricious. More recently, according to the Washington Post, the NSA has gathered 250 million internet communications through Section 702 of the FAA alone, and we also know that the NSA (very quickly) copies and searches communications between “untargeted” individuals to see if they refer to targeted individuals or matters. Both of these facts are strongly suggestive of arbitrariness in a substantive sense: deeply intrusive practices that affect people who are not at all suspected of wrongdoing. The same point stands with respect to the collection of transactional data. Recall Binney’s claims that AT&T simply turned over all of its calling records (in addition to providing wiretap access to ongoing calls), and the reporting in the Wall Street Journal concerning collection of financial data and other private “transactional” details about individuals. We now know that Verizon has been turning over all of its transactional calling data, regardless of whether the data pertain to people who are under suspicion. The Human Rights Committee has taken a position on the collection of such data, stipulating that “. . . the competent public authorities should only be able to call for such information relating to an individual’s private life the knowledge of which is essential in the interests of society as understood under the Covenant.” Untargeted collection of the sort documented above is so broad that it would seem impossible to escape the conclusion that it is arbitrary in the sense defined by Nowak, Volio and the Human Rights Committee.

2. The NSA is engaged in a massive surveillance program—telephone metadata collection, and monitoring of electronic communications on a global scale

American Civil Liberties Union, “United States’ Compliance with the International Covenant on Civil and Political Rights,” *SHADOW REPORT TO THE FOURTH PERIODIC REPORT OF THE UNITED STATES*, 9—13—13, p. 48.

Over the last two months, it has become clear that the National Security Agency (NSA) is engaged in far-reaching, intrusive, and unlawful surveillance of telephone calls and electronic communications both within and outside the United States. Through media reports as well as U.S. government declassifications, we have recently learned about two such forms of NSA surveillance. Through one, the NSA is collecting the “telephone metadata” of every single phone call into, out of, and within the United States. Through another, which includes programs called “PRISM” and “UPSTREAM,” the NSA is engaged in the large-scale collection, storage, and monitoring of the content of electronic communications all around the world. These mass surveillance programs violate the U.S. Constitution and are the product of defects both in the laws that authorize them and in the current oversight system. Both of the programs also raise serious concerns about whether they violate the U.S. government’s obligations under international human rights law to protect the right to privacy and the right to free expression.

Surveillance Undesirable: Privacy—Monitoring of Innocents [cont'd]

3. The NSA is able to surveil virtually everything that happens on the internet

Jonathan Stray, “FAQ: What You Need to Know About the NSA’s Surveillance Programs,” PROPUBLICA, 8—5—13, <http://www.propublica.org/article/nsa-data-collection-faq>, accessed 10-10-13.

The NSA records as much information as it can, subject to technical limitations (there’s a lot of data) and legal constraints. This currently includes the metadata for nearly all telephone calls made in the U.S. (but not their content) and massive amounts of Internet traffic with at least one end outside the U.S. It’s not clear exactly how many cables have been tapped, though we know of at least one inside the U.S., a secret report about the program by the NSA’s Inspector General mentions multiple cables, and the volume of intercepted information is so large that it was processed at 150 sites around the world as of 2008. We also know that Britain’s GCHQ, which shares some intelligence with the NSA, had tapped over 200 cables as of 2012, belonging to seven different telecommunications companies. Until 2011 the NSA also operated a domestic Internet metadata program which collected mass records of who emailed who even if both parties were inside the U.S. Because it is not always possible to separate domestic from foreign communications by automatic means, the NSA still captures some amount of purely domestic information, and it is allowed to do so by the Foreign Intelligence Surveillance Court. The collected information covers “nearly everything a user does on the Internet,” according to a presentation on the XKEYSCORE system. The slides specifically mention emails, Facebook chats, websites visited, Google Maps searches, transmitted files, photographs, and documents of different kinds. It’s also possible to search for people based on where they are connecting from, the language they use, or their use of privacy technologies such as VPNs and encryption, according to the slides.

4. NSA procedures enable the agency to build a massive database about the communications of U.S. citizens

Jameel Jaffer, Deputy Legal Director, ACLU Foundation and Laura W. Murphy, Director, Washington Legislative Office, ACLU, Testimony before the House Judiciary Committee, 7—17—13, <http://judiciary.house.gov/hearings/113th/07172013/Jaffer%2007172913.pdf>, accessed 10-2-13.

The NSA’s procedures permit it to monitor Americans’ international communications in the course of surveillance targeted at foreigners abroad. While the FISA Amendments Act authorizes the government to target foreigners abroad, not Americans, it permits the government to collect Americans’ communications with those foreign targets. The recently disclosed procedures contemplate not only that the NSA will acquire Americans’ international communications but that it will retain them and possibly disseminate them to other U.S. government agencies and foreign governments. Americans’ communications that contain —foreign intelligence information□ or evidence of a crime can be retained forever, and even communications that don’t can be retained for as long as five years. Despite government officials’ claims to the contrary, the NSA is building a growing database of Americans’ international telephone calls and emails.

5. Section 215 collection raises important Fourth Amendment questions

Brennan Center for Justice, New York University School of Law, “Are They Allowed to Do That? A Breakdown of Selected Government Surveillance Programs,” 2013,

www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf, accessed 10-12-13.

It is debatable whether Congress intended the sort of dragnet information collection of phone records that the FISA court has approved under Section 215. Section 215 is dangerously broad, but its plain language does not permit wide-scale surveillance on an ongoing basis. Under the provision, the government is allowed to collect only records that are “relevant” to an authorized investigation. It is difficult to believe that the phone records of millions of Americans are actually “relevant” to a specific terrorist or foreign intelligence investigation. Nor does Section 215 appear to allow the government to collect first and determine relevance later, which is what the government claims it is doing. Even if the government’s actions are consistent with Section 215, the constitutionality of the statute itself is questionable. Some courts have held that the Fourth Amendment’s restriction on searches and seizures means the government must get a warrant to obtain certain types of records, such as cell phone location data. These rulings are at odds with the wide-ranging, warrantless surveillance program that has been allowed under Section 215.

Surveillance Undesirable: Privacy—Section 215 / Metadata

1. The metadata program violates the Fourth Amendment—functions as a general warrant

Laura K. Donohue, Professor, Law, Georgetown University, Testimony before the Senate Judiciary Committee, 10—2—13, <http://www.judiciary.senate.gov/pdf/10-2-13DonohueTestimony.pdf>, accessed 10-8-13.

Consistent with this reading, Professor Akhil Amar, inquiring as to what the warrant clause means—and what the relationship is between it and the earlier reasonableness clause—suggests that “broad warrants—warrants that fail to meet the various specifications of clause two—are inherently unreasonable under clause one.” Such a general warrant would immunize the officer who carried it out from a subsequent trespass suit. In the case of *Entick v. Carrington*, “Armed with sweeping warrants issued by executive officials, various government henchmen broke into Englishmen’s houses, searched their papers, arrested their persons, and rummaged through their effects, in hopes of finding” wrongdoing. Professor Thomas Davies similarly recognizes that “[t]he historical statements about search and seizure” in the fourth Amendment “focused on condemning general warrants. In fact, the historical concerns were almost exclusively about the need to ban house searches under general warrants.” Evidence suggests that “unreasonable searches and seizures” was a proxy for “the inherent illegality of any searches or seizures that might be made under general warrants.” Davies posits that the reason the Framers even bothered “to adopt constitutional bans against general warrants in light of the apparent consensus that the general warrant was illegal at common law” was because of genuine concern that Congress might endanger the right in the future. The FISC Order authorizing the telephony metadata program is, precisely, a general warrant. It authorizes the government to rummage through our papers and effects in the hope of finding wrongdoing. There is no previous suspicion of criminal activity. FISC admits that almost none of the information obtained relates to illegal behavior. It matters little whether one stores ones papers in a filing cabinet in one’s den, or places all financial documents on the iCloud—the digital equivalent, in modern times, of a filing cabinet. Sheer volume of information requires individuals to arrange for storage of everything from medical records to family photos. Email, in turn, holds our correspondence—papers that we place on a server with a company with whom we have a contractual relationship. Banking records may be accessible over the Internet. This is our modern day equivalent of the papers and effects held by *Entick* in his home, and allowing the government to obtain records of all of this information is the equivalent of a digital trespass on our private lives. The trespass in which the NSA is engaging is not supported by probable cause, it is not even supported by reasonable suspicion—indeed, no suspicion of any wrongdoing whatsoever is contemplated by the collection of myriad records of all U.S. persons. It is the equivalent of a general warrant and, as such, is odious to the Fourth Amendment.

2. Metadata collection invades our privacy and violates the Fourth Amendment

Jameel Jaffer, Deputy Legal Director, ACLU Foundation and Laura W. Murphy, Director, Washington Legislative Office, ACLU, Testimony before the House Judiciary Committee, 7—17—13,

<http://judiciary.house.gov/hearings/113th/07172013/Jaffer%2007172913.pdf>, accessed 10-2-13.

President Obama and intelligence officials have been at pains to emphasize that the government is collecting metadata, not content. The suggestion that metadata is somehow beyond the reach of the Constitution, however, is not correct. For Fourth Amendment purposes, the crucial question is not whether the government is collecting content or metadata but whether it is invading reasonable expectations of privacy. In the case of bulk collection of Americans’ phone records, it clearly is. The Supreme Court’s recent decision in *United States v. Jones*, 132 S. Ct. 945 (2012), is instructive. In that case, a unanimous Court held that long-term surveillance of an individual’s location constituted a search under the Fourth Amendment. The Justices reached this conclusion for different reasons, but at least five Justices were of the view that the surveillance infringed on a reasonable expectation of privacy. Justice Sotomayor observed that tracking an individual’s movements over an extended period allows the government to generate a —precise, comprehensive record□ that reflects —a wealth of detail about her familial, political, professional, religious, and sexual associations.□ *Id.* (Sotomayor, J., concurring). The same can be said of the tracking now taking place under Section 215. Call records can reveal personal relationships, medical issues, and political and religious affiliations. Internet metadata may be even more revealing, allowing the government to learn which websites a person visits, precisely which articles she reads, whom she corresponds with, and whom those people correspond with. The long-term surveillance of metadata constitutes a search for the same reasons that the long-term surveillance of location was found to constitute a search in *Jones*. In fact, the surveillance held unconstitutional in *Jones* was narrower and shallower than the surveillance now taking place under Section 215. The location tracking in *Jones* was meant to further a specific criminal investigation into a specific crime, and the government collected information about one person’s location over a period of less than a month. What the government has implemented under Section 215 is an indiscriminate program that has already swept up the communications of millions of people over a period of seven years.

Surveillance Undesirable: Privacy—Section 215 / Metadata [cont'd]

3. Whether the NSA reviews the information is irrelevant—just collecting the data violates the Fourth Amendment

Jameel Jaffer, Deputy Legal Director, ACLU Foundation and Laura W. Murphy, Director, Washington Legislative Office, ACLU, Testimony before the House Judiciary Committee, 7—17—13, <http://judiciary.house.gov/hearings/113th/07172013/Jaffer%2007172913.pdf>, accessed 10-2-13.

Some have defended the metadata program by reference to the Supreme Court's decision in *Smith v. Maryland*, 442 U.S. 735 (1979), which upheld the installation of a pen register in a criminal investigation. The pen register in *Smith*, however, was very primitive—it tracked the numbers being dialed, but it didn't indicate which calls were completed, let alone the duration of the calls. Moreover, the surveillance was directed at a single criminal suspect over a period of less than two days. The police were not casting a net over the whole country. Another argument that has been offered in defense of the metadata program is that, though the NSA collects an immense amount of information, it examines only a tiny fraction of it. But the Fourth Amendment is triggered by the collection of information, not simply by the querying of it. The NSA cannot insulate this program from Fourth Amendment scrutiny simply by promising that Americans' private information will be safe in its hands. The Fourth Amendment exists to prevent the government from acquiring Americans' private papers and communications in the first place.

4. The metadata program is illegal and threatens our privacy

Laura K. Donohue, Professor, Law, Georgetown University, Testimony before the Senate Judiciary Committee, 10—2—13, <http://www.judiciary.senate.gov/pdf/10-2-13DonohueTestimony.pdf>, accessed 10-8-13.

Statutory requirements are designed to protect against the collection of information on U.S. persons. Indeed, the statute limits the scope to obtaining foreign intelligence information “not concerning a United States person”. Where a U.S. person is involved, it must specifically be “to protect against international terrorism or clandestine intelligence activities.” Despite special protections, the collection of information relating to U.S. persons, who are not themselves the target of any investigation, is central to the program. Indeed, from the beginning, both the government and the Court were fully aware that, as a result of the broad approach—namely, the collection of all information, including that of a purely local nature—such information would be obtained. “Ordinarily,” Judge Reggie Walton later wrote, “this alone would provide sufficient grounds for a FISC judge to deny the application.” But in the face of Executive Branch claim, under oath, that the program was vital for U.S. national security, the Court acquiesced, requiring only that the Executive follow certain procedural protections. These protections failed to prevent abuses. The NSA's telephony metadata program contradicts FISA's language, design, and purpose. To understand it otherwise would be to vitiate the statute in terms of Congress' intent in introducing FISA and the general orientation of the statute, as well as the specific statutory restrictions placed on the intelligence agencies and duties assigned to the Foreign Intelligence Surveillance Court. The program also raises constitutional concerns with regard to search and seizure.

5. The metadata program is unconstitutional and should be ended—Fourth Amendment concerns

Laura K. Donohue, Professor, Law, Georgetown University, Testimony before the Senate Judiciary Committee, 10—2—13, <http://www.judiciary.senate.gov/pdf/10-2-13DonohueTestimony.pdf>, accessed 10-8-13.

The NSA's bulk collection of metadata contradicts the general approach adopted by Congress in enacting FISA. The FISC orders lack the particularization required prior to the acquisition of information and the role FISC now plays departs from that envisioned by Congress. The bulk collection program, moreover, violates the statutory language in at least three ways: it does not comport with the requirement that the tangible goods sought “are relevant to an authorized investigation”; it violates the requirement that the information be otherwise obtainable via subpoena duces tecum; and it bypasses the statutory provisions governing pen registers and trap and trace devices. Compounding the illegality of the program are serious constitutional concerns. The FISC order governing the telephony metadata program amounts to a general warrant, which the Fourth Amendment precludes. Efforts by the government to save the program on grounds of third party doctrine are unpersuasive in light of the unique circumstances of *Smith v. Maryland*, new technologies, and changed circumstances. An end to the telephony metadata program and FISA reform are necessary to bring surveillance operations and emerging technologies within the bounds of the Constitution.

Surveillance Undesirable: Privacy—Section 215 / Metadata [cont'd]**6. The metadata program violates FISA—no particularization**

Laura K. Donohue, Professor, Law, Georgetown University, Testimony before the Senate Judiciary Committee, 10—2—13, <http://www.judiciary.senate.gov/pdf/10-2-13DonohueTestimony.pdf>, accessed 10-8-13.

The telephony metadata program violates the general intent of Congress in enacting FISA—and the approach adopted in the statute itself—in two important ways: first, in its rejection of particularization at the point of acquisition of information; and, second, with regard to the role played by the Foreign Intelligence Surveillance Court. A. Particularization in Place of Broad Surveillance The telephony metadata program lacks the particularization that marks Congress' entire approach to domestic foreign intelligence gathering as articulated in the Foreign Intelligence Surveillance Act. Specifically, FISA rejects the wholesale collection of domestic information, insisting instead on minimization; relies on the prior targeting of foreign intelligence targets to justify surveillance; provides U.S. persons a heightened level of protection; and seeks to minimize the acquisition (not just the retention and dissemination) of information.

Surveillance Undesirable: Privacy—Section 702 / PRISM

1. Section 702 raises enormous privacy concerns—allows the government to surveil Americans en masse

Jameel Jaffer, Deputy Legal Director, ACLU Foundation and Laura W. Murphy, Director, Washington Legislative Office, ACLU, Testimony before the House Judiciary Committee, 7—17—13, <http://judiciary.house.gov/hearings/113th/07172013/Jaffer%2007172913.pdf>, accessed 10-2-13.

The ACLU has long expressed deep concerns about the lawfulness of the FISA Amendments Act and surveillance under Section 702. The statute's defects include: * Section 702 allows the government to collect Americans' international communications without requiring it to specify the people, facilities, places, premises, or property to be monitored. Until Congress enacted the FISA Amendments Act, FISA generally prohibited the government from conducting electronic surveillance without first obtaining an individualized and particularized order from the FISA court. In order to obtain a court order, the government was required to show that there was probable cause to believe that its surveillance target was an agent of a foreign government or terrorist group. It was also generally required to identify the facilities to be monitored. The FISA Amendments Act allows the government to conduct electronic surveillance without indicating to the FISA Court whom it intends to target or which facilities it intends to monitor, and without making any showing to the court—or even making an internal executive determination—that the target is a foreign agent or engaged in terrorism. The target could be a human rights activist, a media organization, a geographic region, or even a country. The government must assure the FISA Court that the targets are non-U.S. persons overseas, but in allowing the executive to target such persons overseas, Section 702 allows it to monitor communications between those targets and U.S. persons inside the United States. Moreover, because the FISA Amendments Act does not require the government to identify the specific targets and facilities to be surveilled, it permits the acquisition of these communications en masse. A single acquisition order may be used to justify the surveillance of communications implicating thousands or even millions of U.S. citizens and residents.

2. The program clearly violates the Fourth Amendment

Brennan Center for Justice, New York University School of Law, “Are They Allowed to Do That? A Breakdown of Selected Government Surveillance Programs,” 2013,

www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf, accessed 10-12-13.

The same questions can be raised about PRISM. Like Section 215, Section 702 is remarkably broad, allowing the government to target non-U.S. persons “reasonably believed to be outside the United States.” However, the NSA has reportedly interpreted that to mean that it need only ensure “51 percent confidence of the target’s ‘foreignness.’” Even if the process works as advertised, it could be wrong nearly half the time. Consequently, one of every two people targeted by the NSA may be an American citizen or located in the U.S. The NSA’s training materials call such collection “nothing to worry about.” And even if this practice is deemed consistent with Section 702, it is difficult to see how it comports with the Fourth Amendment, which requires the government to obtain a warrant for much of the information about U.S. persons that is being “inadvertently” collected.

3. PRISM allows the government to track virtually every detail of people’s electronic lives

American Civil Liberties Union, “United States’ Compliance with the International Covenant on Civil and Political Rights,” SHADOW REPORT TO THE FOURTH PERIODIC REPORT OF THE UNITED STATES, 9—13—13, p. 48-49.

The U.S. government’s extensive collection of electronic-communications content under the PRISM and UPSTREAM programs is profoundly disturbing, and it raises serious concerns that the Committee should require the U.S. to address during its upcoming review. The U.S. government has acknowledged that, through PRISM, it may, and does, acquire the contents of the entire digital lives of many people across the globe. In particular, the United States regularly demands emails, audio and video chats, photographs, and other internet traffic from nine major service providers—Microsoft, Yahoo!, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple—located within the United States. The companies are not even allowed to publicly discuss that they received these orders, let alone notify affected individuals whose data has been seized by the U.S. government. Additionally, the media has reported that, under UPSTREAM, the government scans the content of nearly all emails and other text-based communications that enter or leave the United States for particular keywords “about” its foreign-intelligence targets. The PRISM and UPSTREAM programs are authorized by section 702 of the FISA. That statute authorizes the “targeting” of non-U.S. persons reasonably believed to be located outside the United States for foreign-intelligence purposes.

Surveillance Undesirable: Privacy—Section 702 / PRISM [cont'd]

4. Section 702 is not limited to terrorism—can and does cover a wide range of activities

Jameel Jaffer, Deputy Legal Director, ACLU Foundation and Laura W. Murphy, Director, Washington Legislative Office, ACLU, Testimony before the House Judiciary Committee, 7—17—13, <http://judiciary.house.gov/hearings/113th/07172013/Jaffer%2007172913.pdf>, accessed 10-2-13.

Section 702 does not limit government surveillance to communications relating to terrorism. The Act allows the government to conduct dragnet surveillance if a significant purpose of the surveillance is to gather —foreign intelligence information.□ There are multiple problems with this. First, under the new law the —foreign intelligence□ requirement applies to entire surveillance programs, not to individual intercepts. The result is that if a significant purpose of any particular government dragnet is to gather foreign intelligence information, the government can use that dragnet to collect all kinds of communications—not only those that relate to foreign intelligence. Second, the phrase —foreign intelligence information□ has always been defined extremely broadly to include not only information about terrorism but also information about intelligence activities, the national defense, and even the —foreign affairs of the United States.□ Journalists, human rights researchers, academics, and attorneys routinely exchange information by telephone and email that relates to the foreign affairs of the U.S.

5. Section 702 has no real limits on the government power to retain and disseminate information on U.S. citizens

Jameel Jaffer, Deputy Legal Director, ACLU Foundation and Laura W. Murphy, Director, Washington Legislative Office, ACLU, Testimony before the House Judiciary Committee, 7—17—13, <http://judiciary.house.gov/hearings/113th/07172013/Jaffer%2007172913.pdf>, accessed 10-2-13.

Section 702 places no meaningful limits on the government’s retention and dissemination of information relating to U.S. citizens and residents. As a result of the FISA Amendments Act, thousands or even millions of U.S. citizens and residents will find their international telephone and email communications swept up in surveillance that is —targeted□ at people abroad. Yet the law fails to place any meaningful limitations on the government’s retention and dissemination of information that relates to U.S. persons. The law requires the government to adopt —minimization□ procedures—procedures that are —reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons.□ However, these minimization procedures must accommodate the government’s need —to obtain, produce, and disseminate foreign intelligence information.□ In other words, the government may retain or disseminate information about U.S. citizens and residents so long as the information is —foreign intelligence information.□ Because —foreign intelligence information□ is defined broadly (as discussed below), this is an exception that swallows the rule.

6. The NSA uses section 702 to collect significant volumes of citizens’ communications data

Jameel Jaffer, Deputy Legal Director, ACLU Foundation and Laura W. Murphy, Director, Washington Legislative Office, ACLU, Testimony before the House Judiciary Committee, 7—17—13, <http://judiciary.house.gov/hearings/113th/07172013/Jaffer%2007172913.pdf>, accessed 10-2-13.

The metadata program is only one part of the NSA’s domestic surveillance activities. Recent disclosures show that the NSA is also engaged in large-scale monitoring of Americans’ electronic communications under Section 702 of FISA, which codifies the FISA Amendments Act of 2008. Under this program, labeled —PRISM□ in NSA documents, the government collects emails, audio and video chats, photographs, and other internet traffic from nine major service providers—Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube, and Apple. The Director of National Intelligence has acknowledged the existence of the PRISM program but stated that it involves surveillance of foreigners outside the United States. This is misleading. The PRISM program involves the collection of Americans’ communications, both international and domestic, and for reasons explained below, the program is unconstitutional.

Surveillance Undesirable: Privacy—Answers to “Citizens Exempted”

1. Metadata work is used to profile U.S. citizens

James Risen and Laura Poitras, “N.S.A. Gathers Data on Social Connections of U.S. Citizens,” NEW YORK TIMES, 9—28—13, <http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html>, accessed 10-2-13.

The N.S.A. had been pushing for more than a decade to obtain the rule change allowing the analysis of Americans’ phone and e-mail data. Intelligence officials had been frustrated that they had to stop when a contact chain hit a telephone number or e-mail address believed to be used by an American, even though it might yield valuable intelligence primarily concerning a foreigner who was overseas, according to documents previously disclosed by Mr. Snowden. N.S.A. officials also wanted to employ the agency’s advanced computer analysis tools to sift through its huge databases with much greater efficiency. The agency had asked for the new power as early as 1999, the documents show, but had been initially rebuffed because it was not permitted under rules of the Foreign Intelligence Surveillance Court that were intended to protect the privacy of Americans. A 2009 draft of an N.S.A. inspector general’s report suggests that contact chaining and analysis may have been done on Americans’ communications data under the Bush administration’s program of wiretapping without warrants, which began after the Sept. 11 attacks to detect terrorist activities and skirted the existing laws governing electronic surveillance. In 2006, months after the wiretapping program was disclosed by The New York Times, the N.S.A.’s acting general counsel wrote a letter to a senior Justice Department official, which was also leaked by Mr. Snowden, formally asking for permission to perform the analysis on American phone and e-mail data. A Justice Department memo to the attorney general noted that the “misuse” of such information “could raise serious concerns,” and said the N.S.A. promised to impose safeguards, including regular audits, on the metadata program. In 2008, the Bush administration gave its approval. A new policy that year, detailed in “Defense Supplemental Procedures Governing Communications Metadata Analysis,” authorized by Defense Secretary Robert M. Gates and Attorney General Michael B. Mukasey, said that since the Supreme Court had ruled that metadata was not constitutionally protected, N.S.A. analysts could use such information “without regard to the nationality or location of the communicants,” according to an internal N.S.A. description of the policy. After that decision, which was previously reported by The Guardian, the N.S.A. performed the social network graphing in a pilot project for 1 ½ years “to great benefit,” according to the 2011 memo. It was put in place in November 2010 in “Sigint Management Directive 424” (sigint refers to signals intelligence). In the 2011 memo explaining the shift, N.S.A. analysts were told that they could trace the contacts of Americans as long as they cited a foreign intelligence justification. That could include anything from ties to terrorism, weapons proliferation or international drug smuggling to spying on conversations of foreign politicians, business figures or activists.

2. The NSA is failing to ensure that the surveillance targets are foreigners outside of the U.S.

American Civil Liberties Union, HOW THE NSA’S SURVEILLANCE PROCEDURES THREATEN AMERICANS’ PRIVACY, 2013, https://www.aclu.org/files/assets/explainer_v4.pdf, accessed 10-2-13.

2. The Procedures allow the surveillance of Americans by failing to ensure that the NSA’s surveillance targets are in fact foreigners outside the United States. The Act is predicated on the theory that foreigners abroad have no right to privacy—or, at any rate, no right that the United States should respect. Because they have no right to privacy, the U.S. government sees no bar to the collection of their communications, including their communications with Americans. But even if one accepts the government’s premise, the Procedures fail to ensure that the NSA’s surveillance targets are in fact foreigners outside the United States. This is because the Procedures permit the NSA to presume that prospective surveillance targets are foreigners outside the United States absent specific information to the contrary—and to presume therefore that they are fair game for warrantless surveillance.

Surveillance Undesirable: Privacy—Answers to “Citizens Exempted” [cont’d]

3. The NSA is sifting through electronic communications of citizens

Charlie Savage, “N.S.A. Said to Search Content of Messages to and from U.S.,” NEW YORK TIMES, 8—8—13, http://www.nytimes.com/2013/08/08/us/broader-sifting-of-data-abroad-is-seen-by-nsa.html?hp&_r=1&, accessed 10-2-13. The National Security Agency is searching the contents of vast amounts of Americans’ e-mail and text communications into and out of the country, hunting for people who mention information about foreigners under surveillance, according to intelligence officials. The N.S.A. is not just intercepting the communications of Americans who are in direct contact with foreigners targeted overseas, a practice that government officials have openly acknowledged. It is also casting a far wider net for people who cite information linked to those foreigners, like a little used e-mail address, according to a senior intelligence official. While it has long been known that the agency conducts extensive computer searches of data it vacuums up overseas, that it is systematically searching — without warrants — through the contents of Americans’ communications that cross the border reveals more about the scale of its secret operations. It also adds another element to the unfolding debate, provoked by the disclosures of Edward J. Snowden, the former N.S.A. contractor, about whether the agency has infringed on Americans’ privacy as it scoops up e-mails and phone data in its quest to ferret out foreign intelligence. Government officials say the cross-border surveillance was authorized by a 2008 law, the FISA Amendments Act, in which Congress approved eavesdropping on domestic soil without warrants as long as the “target” was a noncitizen abroad. Voice communications are not included in that surveillance, the senior official said.

4. The 2008 amendments mean the programs surveil millions of citizens

Margot Kaminski, Executive Director, Information Society Project, Yale Law School, “PRISM’s Legal Basis: How We Got Here, and What We Can Do to Get Back,” THE ATLANTIC, 6—7—13, www.theatlantic.com/national/archive/2013/06/prisms-legal-basis-how-we-got-here-and-what-we-can-do-to-get-back/276667/, accessed 10-13-13.

The current scope of this “incidental” surveillance will shock most Americans. Before 2008, the law limited “incidental” surveillance by limiting primary surveillance. The government had to show probable cause that its surveillance target was the agent of a foreign power, and that the facility being watched was about to be used by that target. You could be incidentally observed if you communicated with a targeted foreign agent, but otherwise foreign communications were likely to be unmonitored. But in 2008, the FISA Amendments Act (FISAAA) changed this. The government now does not need to show probable cause that the target is a foreign agent. It need only have a “reasonable belief” that the target is located outside of the United States. The new version of FISA does not require the government to identify its targets; it does not require the government to identify the monitored facilities; and the purpose of foreign intelligence gathering attaches to the whole surveillance program, not the individual investigation. That is to say: the FISA Amendments Act permits the government to obtain a single court order through which it can monitor thousands, or even millions, of people. The scope of “incidental” surveillance thus vastly expanded as Congress lowered the requirements for spying on the primary target. Such a system will inevitably sweep in untold numbers of Americans who communicate with foreigners. And because the government need have only a “reasonable belief” that the target is outside the United States—which it is interpreting according to the Washington Post as a 51% chance that the target is outside the U.S.—this system will undoubtedly sweep in purely domestic communications as well.

5. The NSA is collecting information on millions of Americans

American Civil Liberties Union, HOW THE NSA’S SURVEILLANCE PROCEDURES THREATEN AMERICANS’ PRIVACY, 2013, https://www.aclu.org/files/assets/explainer_v4.pdf, accessed 10-2-13.

4. The Procedures permit the NSA to collect international communications, including Americans’ international communications, in bulk. On its face, the Act permits the NSA to conduct dragnet surveillance, not just surveillance of specific individuals. Officials who advocated for the Act made clear that this was one of its principal purposes, and unsurprisingly, the Procedures give effect to that design. While they require the government to identify a “target” outside the country, once the target has been identified the Procedures permit the NSA to sweep up the communications of any foreigner who may be communicating “about” the target. The Procedures contemplate that the NSA will do this by “employ[ing] an Internet Protocol filter to ensure that the person from whom it seeks to obtain foreign intelligence information is located overseas,” by “target[ing] Internet links that terminate in a foreign country,” or by identifying “the country code of the telephone number.” However the NSA does it, the result is the same: millions of communications may be swept up, Americans’ international communications among them.

Surveillance Undesirable: Privacy—Answers to “Citizens Exempted” [cont’d]

6. The NSA is surveiling enormous quantities of citizens’ communications data

Jonathan Stray, “FAQ: What You Need to Know About the NSA’s Surveillance Programs,” PROPUBLICA, 8—5—13, <http://www.propublica.org/article/nsa-data-collection-faq>, accessed 10-10-13.

We don’t know all of the different types of information the NSA collects, but several secret collection programs have been revealed: A record of most calls made in the U.S., including the telephone number of the phones making and receiving the call, and how long the call lasted. This information is known as “metadata” and doesn’t include a recording of the actual call (but see below). This program was revealed through a leaked secret court order instructing Verizon to turn over all such information on a daily basis. Other phone companies, including AT&T and Sprint, also reportedly give their records to the NSA on a continual basis. All together, this is several billion calls per day. Email, Facebook posts and instant messages for an unknown number of people, via PRISM, which involves the cooperation of at least nine different technology companies. Google, Facebook, Yahoo and others have denied that the NSA has “direct access” to their servers, saying they only release user information in response to a court order. Facebook has revealed that, in the last six months of 2012, they handed over the private data of between 18,000 and 19,000 users to law enforcement of all types -- including local police and federal agencies, such as the FBI, Federal Marshals and the NSA. Massive amounts of raw Internet traffic The NSA intercepts huge amounts of raw data, and stores billions of communication records per day in its databases. Using the NSA’s XKEYSCORE software, analysts can see “nearly everything a user does on the Internet” including emails, social media posts, web sites you visit, addresses typed into Google Maps, files sent, and more. Currently the NSA is only authorized to intercept Internet communications with at least one end outside the U.S., though the domestic collection program used to be broader. But because there is no fully reliable automatic way to separate domestic from international communications, this program also captures some amount of U.S. citizens’ purely domestic Internet activity, such as emails, social media posts, instant messages, the sites you visit and online purchases you make. The contents of an unknown number of phone calls There have been several reports that the NSA records the audio contents of some phone calls and a leaked document confirms this. This reportedly happens “on a much smaller scale” than the programs above, after analysts select specific people as “targets.” Calls to or from U.S. phone numbers can be recorded, as long as the other end is outside the U.S. or one of the callers is involved in “international terrorism”. There does not seem to be any public information about the collection of text messages, which would be much more practical to collect in bulk because of their smaller size. The NSA has been prohibited from recording domestic communications since the passage of the Foreign Intelligence Surveillance Act but at least two of these programs -- phone records collection and Internet cable taps -- involve huge volumes of Americans’ data.

7. The NSA often does not need a warrant to search through specific persons’ data

Jonathan Stray, “FAQ: What You Need to Know About the NSA’s Surveillance Programs,” PROPUBLICA, 8—5—13, <http://www.propublica.org/article/nsa-data-collection-faq>, accessed 10-10-13.

It’s complicated, but not in all cases. Leaked court orders set out the “minimization” procedures that govern what the NSA can do with the domestic information it has intercepted. The NSA is allowed to store this domestic information because of the technical difficulties in separating foreign from domestic communications when large amounts of data are being captured. Another document shows that individual intelligence analysts make the decision to look at previously collected bulk information. They must document their request, but only need approval from their “shift coordinator.” If the analyst later discovers that they are looking at the communications of a U.S. person, they must destroy the data. However, if the intercepted information is “reasonably believed to contain evidence of a crime” then the NSA is allowed to turn it over to federal law enforcement. Unless there are other (still secret) restrictions on how the NSA can use this data this means the police might end up with your private communications without ever having to get approval from a judge, effectively circumventing the whole notion of probable cause. This is significant because thousands or millions of people might fall into the extended social network of a single known target, but it is not always possible to determine whether someone is a U.S. person before looking at their data. For example, it’s not usually possible to tell just from someone’s email address, which is why the NSA maintains a database of known U.S. email addresses and phone numbers. Internal documents state that analysts need only “51% confidence” that someone is a non-U.S. person before looking at their data, and if the NSA does not have “specific information” about someone, that person is “presumed to be a non-United States person.” Also, the NSA is allowed to provide any of its recorded information to the FBI, if the FBI specifically asks for it.

Surveillance Undesirable: Privacy—Answers to “Info Not Shared”**- Sharing information is irrelevant—we should be able to control who gets our information**

Jameer Jaffer, fellow, Open Society Foundations, “Secrecy and Freedom,” NEW YORK TIMES, Room for Debate, 6—9—13, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined>, accessed 10-4-13.

Of course we share personal information with government agents all the time. We share financial information with the I.R.S., we share information about our children with public school teachers, and so on. But the fact that we sometimes share discrete categories of information with specific categories of people for narrowly delineated purposes doesn’t seem to me to be very relevant. “Privacy” means being able to decide for ourselves whom our information is shared with, and when, and under what conditions. The chilling effect of surveillance makes our public debates narrower and more inhibited and our democracy less vital. Needless to say, the right of privacy shouldn’t trump everything. National security (and other government interests) may justify some narrow intrusions on privacy in some circumstances. The problem with the programs disclosed over last week is that they are so astonishingly broad.

Surveillance Undesirable: Privacy—Answers to “Intel Only”

1. Federal definitions of ‘intelligence’ leave virtually every electronic communication around the globe subject to extra-judicial NSA surveillance

American Civil Liberties Union, “United States’ Compliance with the International Covenant on Civil and Political Rights,” SHADOW REPORT TO THE FOURTH PERIODIC REPORT OF THE UNITED STATES, 9—13—13, p. 49.

Even though the law requires judicial approval before the government can engage in this kind of surveillance, in practice, there is little judicial involvement in the program. By making an application to the FISC, the U.S. government may obtain a mass-acquisition order that authorizes, for an entire year, whatever surveillance the government may choose to engage in, within broadly drawn parameters. Additionally, the government’s definition of “foreign intelligence” sweeps so broadly that it potentially encompasses almost any foreign person at all—not just individuals who are foreign agents, engaged in criminal activity, or connected even remotely with terrorist activities. Finally, the U.S. government’s targeting procedures allow the NSA to sweep up the communications of not only any foreigner who is a target, but any foreigner who may be communicating about the target as well. The effect of this expansive scheme is to bring virtually every international communication within the reach of the NSA’s surveillance. What’s more, the government retains most of the information it collects under section 702 indefinitely, and it may disseminate and analyze collected information with only limited restrictions. Moreover, it may do so without subjecting itself to the scrutinizing glare of the courts.

2. The NSA is conducting surveillance outside of its “foreign intelligence” mandate

American Civil Liberties Union, HOW THE NSA’S SURVEILLANCE PROCEDURES THREATEN AMERICANS’ PRIVACY, 2013, https://www.aclu.org/files/assets/explainer_v4.pdf, accessed 10-2-13.

3. The Procedures permit the government to conduct surveillance that has no real connection to the government’s foreign intelligence interests. One of the fundamental problems with the Act is that it permits the government to conduct surveillance without probable cause or individualized suspicion. It permits the government to monitor people who aren’t even thought to be doing anything wrong, and to do so without particularized warrants or meaningful review by impartial judges. Government officials have placed heavy emphasis on the fact that the Act allows the government to conduct surveillance only if one of its purposes is to gather “foreign intelligence information.” That term, though, is defined very broadly to include not only information about terrorism but also information about intelligence activities, the national defense, and even “the foreign affairs of the United States.” The Procedures weaken the limitation further. Among the things the NSA examines to determine whether a particular email address or phone number will be used to exchange foreign intelligence information is whether it has been used in the past to communicate with foreigners. Another is whether it is listed in a foreigner’s address book. In other words, the NSA seems to equate a propensity to communicate with foreigners with a propensity to communicate foreign intelligence information. The effect is to bring virtually every international communication within the reach of the NSA’s surveillance.

3. Section 702 surveillance powers are so broad that they often have nothing to do with ‘foreign intelligence’

Jameel Jaffer, Deputy Legal Director, ACLU Foundation and Laura W. Murphy, Director, Washington Legislative Office, ACLU, Testimony before the House Judiciary Committee, 7—17—13, <http://judiciary.house.gov/hearings/113th/07172013/Jaffer%2007172913.pdf>, accessed 10-2-13.

The NSA’s procedures permit the government to conduct surveillance that has no real connection to the government’s foreign intelligence interests. One of the fundamental problems with Section 702 is that it permits the government to conduct surveillance without probable cause or individualized suspicion. It permits the government to monitor people who are not even thought to be doing anything wrong, and to do so without particularized warrants or meaningful review by impartial judges. Government officials have placed heavy emphasis on the fact that the FISA Amendments Act allows the government to conduct surveillance only if one of its purposes is to gather —foreign intelligence information. □ As noted above, however, that term is defined very broadly to include not only information about terrorism but also information about intelligence activities, the national defense, and even —the foreign affairs of the United States. □ The NSA’s procedures weaken the limitation further. Among the things the NSA examines to determine whether a particular email address or phone number will be used to exchange foreign intelligence information is whether it has been used in the past to communicate with foreigners. Another is whether it is listed in a foreigner’s address book. In other words, the NSA appears to equate a propensity to communicate with foreigners with a propensity to communicate foreign intelligence information. The effect is to bring virtually every international communication within the reach of the NSA’s surveillance.

Surveillance Undesirable: Privacy—Answers to “Internal Safeguards”

1. NSA abuses are likely—lack of oversight, and the agency itself covers up mistakes and exaggerates threats to expand its power and influence

Jay Stanley, Senior Policy Analyst, ACLU Speech, Privacy & Technology Project, “The National Security State: Why It’s Important to Understand the Nature of the Beast,” FREE FUTURE, American Civil Liberties Union, 9—10—13, <https://www.aclu.org/blog/criminal-law-reform-national-security-technology-and-liberty/national-security-state-why-its>, accessed 10-8-13.

To begin with, if policymakers and the public have a sophisticated understanding of what I called the “Sorcerer’s Apprentice” nature of any agencies we create or maintain, we’re more likely to put in place the right kinds of tight controls and limits to ensure that the agency doesn’t run amok. We’ll be more likely to anticipate the areas in which the agency will likely seek to expand its authorities, to exaggerate problems, to try poaching the domains of adjoining agencies, to escape oversight through secrecy, and so forth—and to craft laws and policies to counteract those tendencies. Many people with long experience in Washington already understand these dynamics at one level or another—but many other people are very naïve about them. If an agency says there’s a “missile gap” with the Soviets, or warns about imminent “cyber-terrorism” leading to blood on the streets, or pushes for judges to be cut out of the equation when surveillance orders are generated, it does not occur to many people that these claims may reflect the natural tendency of government agencies to seek expanded powers, domains, and budgets. Many people, when they feel warm and fuzzy about a president, therefore feel warm and fuzzy about all the agencies that, they think, are under that president’s control—and when they hate and distrust a president, they likewise hate and distrust the agencies. So a good understanding of the nature of the beast will help introduce a healthy skepticism towards many of the claims that government agencies make, and an understanding that they are bigger than the personalities of any of their leaders. The dynamics I talked about probably apply to any bureaucracy, and as a result it is important to put in place realistic oversight and checks and balances whether we’re talking about the NSA or the Department of Housing and Urban Development. But when we’re dealing with the national security agencies, it’s doubly important that we put in place such controls. First, when mistakes are made in the national security arena, the stakes are higher: people die, human rights are violated, and Americans’ privacy and civil liberties are destroyed. Second, the wall of secrecy behind which our national security agencies operate has the effect of magnifying all the problems that I have talked about. If bureaucracies are prone to do whatever it takes to increase their own scope and power, how much worse the problem is when they can selectively hide and release information in order to promote that agenda, manipulating the very broad secrecy powers they’ve been given in the name of protecting us all. So oversight over national security-related agencies has to be better, not worse than that imposed on the average bureaucracy. Yet we have seen just the opposite. Our security agencies have been granted vast deference, their self-serving claims about various threats and dangers all too often taken at face value—and they have been allowed to hide behind secrecy powers far more sweeping than necessary to serve our true national interest.

2. NSA safeguards are a joke—they do not even ensure that the targets of communication are even foreigners

Jameel Jaffer, Deputy Legal Director, ACLU Foundation and Laura W. Murphy, Director, Washington Legislative Office, ACLU, Testimony before the House Judiciary Committee, 7—17—13, <http://judiciary.house.gov/hearings/113th/07172013/Jaffer%2007172913.pdf>, accessed 10-2-13.

The NSA’s procedures allow the surveillance of Americans by failing to ensure that its surveillance targets are in fact foreigners outside the United States. The FISA Amendments Act is predicated on the theory that foreigners abroad have no right to privacy—or, at any rate, no right that the United States should respect. Because they have no right to privacy, the NSA sees no bar to the collection of their communications, including their communications with Americans. But even if one accepts this premise, the NSA’s procedures fail to ensure that its surveillance targets are in fact foreigners outside the United States. This is because the procedures permit the NSA to presume that prospective surveillance targets are foreigners outside the United States absent specific information to the contrary—and to presume therefore that they are fair game for warrantless surveillance.

Surveillance Undesirable: Privacy—Answers to “Internal Safeguards” [cont’d]

3. The NSA repeatedly violates its own rules

Thomas R. Eddlem, “The NSA Domestic Surveillance Lie,” *NEW AMERICAN*, 9—22—13, www.thenewamerican.com/usnews/politics/item/16580-the-nsa-domestic-surveillance-lie, accessed 10-13-13.

In a televised interview on July 18, 2013, NSA Director General Alexander admitted that the NSA does collect the “content” of Americans’ personal communications but, he insisted, the government is not listening to or sifting through the collection of data on Americans. The NSA has safeguards against actually searching Americans’ data. NBC Reporter Pete Williams: “Let’s talk about the phone program. You gather all this data from the phone companies and it sits in your big tank. What can you do? Can you munch on it and chew on it and do data mining, or does it just sit there until you have some specific question?” Gen. Alexander: “Yeah, it sits there. And that’s a great question because the court restricts what we can do with that data. We can only look at that data if we have a nexus to al-Qaida or other terrorist groups.” This was the fallback position of the Obama administration throughout the month of July. They essentially claimed that the NSA was collecting all types of data on Americans, but that this collection is put into a type of legal lockbox that is not touched without a warrant and a court order from a FISA court. But by August 15, the *Washington Post* had reported that the NSA had violated the privacy of Americans’ data — and had violated its own rules — thousands of times per year. Thus, the Obama administration was forced to fall back to the next lie, that the NSA had never intentionally violated Americans’ privacy by searching their private e-mails and phone records.

4. Internal NSA provisions do nothing to protect citizens’ privacy

Jameel Jaffer, Deputy Legal Director, ACLU Foundation and Laura W. Murphy, Director, Washington Legislative Office, ACLU, Testimony before the House Judiciary Committee, 7—17—13, <http://judiciary.house.gov/hearings/113th/07172013/Jaffer%2007172913.pdf>, accessed 10-2-13.

Since the FISA Amendments Act was enacted in 2008, the government’s principal defense of the law has been that —targeting□ and —minimization□ procedures supply sufficient protection for Americans’ privacy. Because the procedures were secret, the government’s assertion was impossible to evaluate. Now that the procedures have been published, however, it is plain that the assertion is false. Indeed, the procedures confirm what critics have long suspected—that the NSA is engaged in unconstitutional surveillance of Americans’ communications, including their telephone calls and emails. The documents show that the NSA is conducting sweeping surveillance of Americans’ international communications, that it is acquiring many purely domestic communications as well, and that the rules that supposedly protect Americans’ privacy are weak and riddled with exceptions.

5. Safeguards are inadequate—an internal audit shows that the NSA is violating its own rules

Scott Lemieux, Assistant Professor, Political Science, College of Saint Rose, “The NSA Can’t Be Trusted,” *AMERICAN PROSPECT*, 8—19—13, <http://prospect.org/article/nsa-cant-be-trusted>, accessed 10-8-13.

On August 9, President Obama gave a news conference at which he defended his administration’s record on surveillance while proposing some modest reforms. Predictably, it got mixed reviews from observers concerned about civil liberties. Less than a week later, *The Washington Post* published an important story about the National Security Agency (NSA) that makes it clear more reforms are necessary—and undermine Obama’s defense of his record. The key finding of the story, by Scott Wilson and Zachary Goldfarb: An internal audit found 2,776 “incidents” in which NSA surveillance breached rules between April 2011 and March 2012. Even worse, the rates of illegal “incidents” have been increasing. As the *Post*’s Timothy Lee says, “We now know that President Obama’s assurances that the NSA wasn’t ‘actually abusing’ its surveillance programs are untrue.” The only question is whether Obama deliberately misled the public, or whether he was unaware of these violations. Neither possibility is very encouraging.

Surveillance Undesirable: Privacy—Answers to “Internal Safeguards” [cont’d]**6. A low “incidence of violation” rate is irrelevant—the privacy concerns are real and will only increase as the NSA expands its programs**

Scott Lemieux, Assistant Professor, Political Science, College of Saint Rose, “The NSA Can’t Be Trusted,” AMERICAN PROSPECT, 8—19—13, <http://prospect.org/article/nsa-cant-be-trusted>, accessed 10-8-13.

The second line of defense, however, is less persuasive. The NSA argues in the Post story that the violations need to be viewed in the context of the total number of searches conducted by the NSA: “You can look at it as a percentage of our total activity that occurs each day,” he said. “You look at a number in absolute terms that looks big, and when you look at it in relative terms, it looks a little different.” Viewing the violations in relative terms is relevant if we’re evaluating the good faith of the agents within the NSA. In broader civil liberties terms, however, to focus on relative as opposed to absolute numbers is wrong. Precisely the problem with moving away from the typical requirement that searches and seizures require individualized suspicion is that the sheer scope of the NSA’s searches increases the chances for violations of civil liberties. That the large number of violations occurred in the context of a huge number of searches is beside the point. The more searches, the greater the chances civil liberties violations will occur. Indeed, in this sense the fact that most of the errors seem to have been inadvertent is even more disturbing—if this number of violations can occur when agents are trying to follow the law in good faith, consider the dangers posed by NSA personnel who aren’t acting in good faith.

Surveillance Undesirable: Privacy—Answers to “Limited Data Timeframe”

1. The current program creates a permanent database that allows the NSA to track the activity of any citizen

Kate Martin, Center for National Security Studies, Testimony before the House Judiciary Committee, 7—17—13, <http://judiciary.house.gov/hearings/113th/07172013/Martin%2007172013.pdf>, accessed 10-2-13.

A key purpose of the Fourth Amendment was to prevent general searches by the government. This was accomplished in part through the Amendment’s requirement of particularity -- that the target of a search or seizure, the place to be searched, the things to be seized all had to be specifically identified in a warrant issued by a judge. We now face the situation where the government has the capacity to collect massive amounts of information on millions of Americans, to store that information indefinitely, and to analyze that information to discover enormous amounts of revealing information about individual Americans’ private lives and political activities. As others have demonstrated, the underlying rationales for the old distinctions between content and meta-data, or the notion that Fourth Amendment protections have no applicability to information about an individual held by third parties, no longer hold in the new world of massive electronic data about individuals held by Internet service providers, telecommunications companies and others. At the same time, there has been a fundamental shift in the way that the government collects information on Americans. The two sections of FISA that have been the focus of the leaks, 50 U.S.C. § 1861, 1881a, “sections 215 and 702”, are apparently used by the government to obtain information about thousands of communications of Americans, but without even any suspicion about the individual Americans whose communications are being collected. To the contrary, these authorities are apparently being used for en masse bulk collection on thousands or millions of individuals without any individualized showing of suspicion about any party to the communication, whether American or foreigner. While it is true that the NSA has had such bulk collection capabilities for many years, those capabilities were aimed overseas and their purpose was to collect information about foreign governments and foreign terrorist organizations. That collection did include “incidentally acquired” information on Americans’ communications, but that was not the purpose of the collection, and there were strict rules about the NSA disseminating that information to other government agencies for their use. Nor, as far as we know, was the government creating massive databases on Americans’ communications as an integral part of its “foreign intelligence” activities.

2. The NSA is retaining Americans’ communications data with foreigners, and will be able to review them in the future

American Civil Liberties Union, HOW THE NSA’S SURVEILLANCE PROCEDURES THREATEN AMERICANS’ PRIVACY, 2013, https://www.aclu.org/files/assets/explainer_v4.pdf, accessed 10-2-13.

1. The Procedures permit the NSA to monitor Americans’ international communications in the course of surveillance targeted at foreigners abroad. The NSA “is not listening to Americans’ phone calls or monitoring their emails,” the Chairman of the House Intelligence Committee recently said, and many other government officials, including the president himself, have made similar assurances. But these statements are not true. While the FISA Amendments Act authorizes the government to target foreigners abroad, not Americans, it permits the government to collect Americans’ communications with those foreign targets. Indeed, in advocating for the Act, government officials made clear that these “one-end-domestic” communications were the ones of most interest to them. The Procedures contemplate not only that the NSA will acquire Americans’ international communications but that it will retain them and possibly disseminate them to other U.S. government agencies and foreign governments. Americans’ communications that contain “foreign intelligence information” or evidence of a crime can be retained forever, and even communications that don’t can be retained for as long as five years. Despite government officials’ claims to the contrary, the NSA is building a growing database of Americans’ international telephone calls and emails.

3. The NSA can keep domestic data for up to five years, and store encrypted data indefinitely

Jonathan Stray, “FAQ: What You Need to Know About the NSA’s Surveillance Programs,” PROPUBLICA, 8—5—13, <http://www.propublica.org/article/nsa-data-collection-faq>, accessed 10-10-13.

The NSA can generally keep intercepted domestic communications for up to five years. It can keep them indefinitely under certain circumstances, such as when the communication contains evidence of a crime or when it’s “foreign intelligence information,” a broad legal term that includes anything relevant to “the conduct of the foreign affairs of the United States.” The NSA can also keep encrypted communications indefinitely. That includes any information sent to or from a secure web site, that is, a site with a URL starting with “https”.

Surveillance Undesirable: Privacy—Answers to “Limited Data Timeframe” [cont’d]

4. The NSA is collecting enormous volumes of information that it will keep for years

James Risen and Laura Poitras, “N.S.A. Gathers Data on Social Connections of U.S. Citizens,” NEW YORK TIMES, 9—28—13, <http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html>, accessed 10-2-13.

The N.S.A. documents show that one of the main tools used for chaining phone numbers and e-mail addresses has the code name Mainway. It is a repository into which vast amounts of data flow daily from the agency’s fiber-optic cables, corporate partners and foreign computer networks that have been hacked. The documents show that significant amounts of information from the United States go into Mainway. An internal N.S.A. bulletin, for example, noted that in 2011 Mainway was taking in 700 million phone records per day. In August 2011, it began receiving an additional 1.1 billion cellphone records daily from an unnamed American service provider under Section 702 of the 2008 FISA Amendments Act, which allows for the collection of the data of Americans if at least one end of the communication is believed to be foreign. The overall volume of metadata collected by the N.S.A. is reflected in the agency’s secret 2013 budget request to Congress. The budget document, disclosed by Mr. Snowden, shows that the agency is pouring money and manpower into creating a metadata repository capable of taking in 20 billion “record events” daily and making them available to N.S.A. analysts within 60 minutes. The spending includes support for the “Enterprise Knowledge System,” which has a \$394 million multiyear budget and is designed to “rapidly discover and correlate complex relationships and patterns across diverse data sources on a massive scale,” according to a 2008 document. The data is automatically computed to speed queries and discover new targets for surveillance. A top-secret document titled “Better Person Centric Analysis” describes how the agency looks for 94 “entity types,” including phone numbers, e-mail addresses and IP addresses. In addition, the N.S.A. correlates 164 “relationship types” to build social networks and what the agency calls “community of interest” profiles, using queries like “travelsWith, hasFather, sentForumMessage, employs.” A 2009 PowerPoint presentation provided more examples of data sources available in the “enrichment” process, including location-based services like GPS and TomTom, online social networks, billing records and bank codes for transactions in the United States and overseas. At a Senate Intelligence Committee hearing on Thursday, General Alexander was asked if the agency ever collected or planned to collect bulk records about Americans’ locations based on cellphone tower data. He replied that it was not doing so as part of the call log program authorized by the Patriot Act, but said a fuller response would be classified. If the N.S.A. does not immediately use the phone and e-mail logging data of an American, it can be stored for later use, at least under certain circumstances, according to several documents. One 2011 memo, for example, said that after a court ruling narrowed the scope of the agency’s collection, the data in question was “being buffered for possible ingest” later. A year earlier, an internal briefing paper from the N.S.A. Office of Legal Counsel showed that the agency was allowed to collect and retain raw traffic, which includes both metadata and content, about “U.S. persons” for up to five years online and for an additional 10 years offline for “historical searches.”

5. Our capacity to store and analyze metadata is growing rapidly

Danielle Keats Citron and David Gray, University of Maryland School of Law, “Addressing the Harm of Total Surveillance: A Reply to Professor Neil Richards,” HARVARD LAW REVIEW FORUM v. 126, 2013, p. 265.

The scope of surveillance capacities continues to grow. Fusion centers and projects like Virtual Alabama may already have access to broadband providers’ deep packet inspection (DPI) technologies, which store and examine consumers’ online activities and communications. This would provide government and private collaborators with a window into online activities, which could then be exploited using data-mining and statistical-analysis tools capable of revealing more about us and our lives than we are willing to share with even intimate family members. More unsettling still is the potential combination of surveillance technologies with neuroanalytics to reveal, predict, and manipulate instinctual behavioral patterns of which we are not even aware.

Surveillance Undesirable: Privacy—Answers to “Metadata Ignores Content”

1. Content can readily be inferred from metadata

Edward W. Felten, Professor, Computer Science and Public Affairs, Princeton University, Testimony before the Senate Intelligence Committee, 10—2—13, <http://www.judiciary.senate.gov/pdf/10-2-13FeltenTestimony.pdf>, accessed 10-8-13. Telephony metadata can be extremely revealing, both at the level of individual calls and, especially, in the aggregate. Although this metadata might, on first impression, seem to be little more than “information concerning the numbers dialed,” analysis of telephony metadata often reveals information that could traditionally only be obtained by examining the contents of communications. That is, metadata is often a proxy for content. In the simplest example, certain telephone numbers are used for a single purpose, such that any contact reveals basic and often sensitive information about the caller. Examples include support hotlines for victims of domestic violence and rape. Similarly, numerous hotlines exist for people considering suicide, including specific services for first responders, veterans, and gay and lesbian teenagers. Hotlines exist for sufferers of various forms of addiction, such as alcohol, drugs, and gambling. Similarly, inspectors general at practically every federal agency—including the NSA²⁶—have hotlines through which misconduct, waste, and fraud can be reported, while numerous state tax agencies have dedicated hotlines for reporting tax fraud. Hotlines have also been established to report hate crimes, arson, illegal firearms and child abuse. In all these cases, the metadata alone conveys a great deal about the content of the call, even without any further information. The phone records indicating that someone called a sexual assault hotline or a tax fraud reporting hotline will of course not reveal the exact words that were spoken during those calls, but phone records indicating a 30-minute call to one of these numbers will still reveal information that virtually everyone would consider extremely private. In some cases, metadata is even more sensitive than the contents of a communication. For example, wireless telephone carriers permit subscribers to donate to certain charities by sending a text message from their mobile phones. These systems require the subscriber to send a specific text message to a special number, which will then cause the wireless carrier to add that donation to the subscriber’s monthly telephone bill. For example, by sending the word HAITI to 90999, a wireless subscriber can donate \$10 to the American Red Cross.

2. The NSA programs target individuals, including citizens

John Prados, senior fellow, National Security Archive, “Demystifying the NSA Surveillance Program,” HISTORY NEWS NETWORK, 7—15—13, <http://hnn.us/article/152605>, accessed 10-13-13.

The types of information collected are said to include the times and dates of phone calls, volume and duration, phone numbers, and location of originating and destination points. These are called “metadata.” Citizens are supposed to be reassured that no one is listening in. Functionally speaking such items can be called the “externals” surrounding message content. In two world wars and many other conflicts the external elements of communications formed the basis for “traffic analysis,” which has been viewed as the glue that held together radio intelligence when codebreakers were not actually decrypting message content. In World War II, Korea, Vietnam, and elsewhere, traffic analysis identified superiors and subordinates, chains of command, movements to concentrate, and more. A key purpose of traffic analysis was to discover targets. The enemies then were nation states, but the target set of NSA eavesdropping today has expanded to include citizens. That citizens are targets ought to worry every individual, especially since the explicitly-stated purpose of the spying is to protect them.

3. Regular citizens have no protection against this metadata approach

John Prados, senior fellow, National Security Archive, “Demystifying the NSA Surveillance Program,” HISTORY NEWS NETWORK, 7—15—13, <http://hnn.us/article/152605>, accessed 10-13-13.

The term of art is “communications security” or comsec. This starts with staying off the radio, or phone, and progresses through the use of voice codes, sophisticated scrambling or encryption systems, frequency-alternating devices, and the like. The latest is the blind email deposit box. Save for the first and last-named techniques, these alternatives are available primarily to states, hardly to citizens. Al Qaeda learned comsec very early. After about mid-2003 electronic monitoring became increasingly ineffective against them. Bin Laden is known to have maintained telephone silence for years. Traffic analysis offered some potential over a longer period—and no doubt this is a reason why the United States became so enamored of the eavesdropping. But the terrorist enemy has been worn down while the metadata vacuuming continues at an even higher rate, against individual citizens who have no protection.

Surveillance Undesirable: Privacy—Answers to “Metadata Ignores Content” [cont’d]

4. Criminal suspicion loopholes open the door to massive citizen surveillance

John Prados, senior fellow, National Security Archive, “Demystifying the NSA Surveillance Program,” HISTORY NEWS NETWORK, 7—15—13, <http://hnn.us/article/152605>, accessed 10-13-13.

Once the citizen is identified as a target the authorities do have the legal means to go beyond metadata and intrude on actual content, by applying standard FISA procedures. The Foreign Intelligence Surveillance Court (FISC) issues a warrant and then the common carriers—the internet and phone companies—furnish the NSA with content, written and audio-visual. The latest revelations in the NSA scandal show that even comsec does not work—Microsoft provided the agency with pre-encrypted materials (what the codebreakers call “clear text”) even for its chat rooms and message systems that have encryption features, as well as access to cloud storage systems with millions of users. The greater danger to the citizen is not terrorism as probable cause before the Court but the additional rationale written into the law, covering suspicion of any criminal activity. The criminal activity provision suspends protections in the protocols that might otherwise shield American citizens. Suspicion of criminal activity opens a huge spectrum since it involves federal law, from immigration to tax evasion, from violations of fair housing, employment or sports statutes to suspected leaking of classified information.

5. Metadata is not anonymous—can be used to identify people and behavior, and it raises serious potential for abuse

Jonathan Stray, “FAQ: What You Need to Know About the NSA’s Surveillance Programs,” PROPUBLICA, 8—5—13, <http://www.propublica.org/article/nsa-data-collection-faq>, accessed 10-10-13.

Even without the content of all your conversations and text messages, so-called “metadata” can reveal a tremendous amount about you. If they have your metadata, the NSA would have a record of your entire address book, or at least every person you’ve called in the last several years. They can guess who you are close to by how often you call someone, and when. By correlating the information from multiple people, they can do sophisticated “network analysis” of communities of many different kinds, personal or professional -- or criminal. Phone company call records reveal where you were at the time that a call was made, because they include the identifier of the radio tower that transmitted the call to you. The government has repeatedly denied that it collects this information, but former NSA employee Thomas Drake said they do. For a sense of just how powerful location data can be, see this visualization following a German politician everywhere he goes for months, based on his cellphone’s location information. Even without location data, records of who communicated with whom can be used to discover the structure of groups planning terrorism. Starting from a known “target” (see above), analysts typically reconstruct the social network “two or three hops” out, examining all friends-of-friends, or even friends-of-friends-of-friends, in the search for new targets. This means potentially thousands or millions of people might be examined when investigating a single target. Metadata is a sensitive topic because there is great potential for abuse. While no one has claimed the NSA is doing this, it would be possible to use metadata to algorithmically identify, with some accuracy, members of other types of groups like the Tea Party or Occupy Wall Street, gun owners, undocumented immigrants, etc. An expert in network analysis could start with all of the calls made from the time and place of a protest, and trace the networks of associations out from there. Phone metadata is also not “anonymous” in any real sense. The NSA already maintains a database of the phone numbers of all Americans for use in determining whether someone is a “U.S. person” (see below), and there are several commercial number-to-name services in any case. Phone records become even more powerful when they are correlated with other types of data, such as social media posts, local police records and credit card purchase information, a process known as intelligence fusion.

Surveillance Undesirable: Privacy—Answers to “Metadata Ignores Content” [cont’d]

6. Metadata can be used to track our social relationships, build maps of organizations

Edward W. Felten, Professor, Computer Science and Public Affairs, Princeton University, Testimony before the Senate Intelligence Committee, 10—2—13, <http://www.judiciary.senate.gov/pdf/10-2-13FeltenTestimony.pdf>, accessed 10-8-13. When call metadata is aggregated and mined for information across time, it can be an even richer repository of personal and associational details. Metadata can identify our closest relationships. Two people in an intimate relationship may regularly call each other, often late in the evening. If those calls become less frequent or end altogether, metadata will tell us that the relationship has likely ended as well—and it will tell us when a new relationship gets underway. More generally, someone you speak to once a year is less likely to be a close friend than someone you talk to once a week. Analysis of metadata on this scale can reveal the network of individuals with whom we communicate—commonly called a social graph. Metadata also reveals the structure and activities of organizations. By building a social graph that maps all of an organization’s telephone calls over time, one could obtain a set of contacts that includes a substantial portion of the organization’s membership, donors, political supporters, and so on. Analysis of the metadata belonging to these individual callers, by moving one “hop” further out, could help to classify each one, eventually yielding a detailed breakdown of the organization’s associational relationships. Even our relative power and social status can be determined by calling patterns. As *The Economist* observed in 2010, “People at the top of the office or social pecking order often receive quick callbacks, do not worry about calling other people late at night and tend to get more calls at times when social events are most often organized (sic), such as Friday afternoons.” At times, by placing multiple calls in context, metadata analysis can even reveal patterns and sensitive information that would not be discoverable by intercepting the content of an individual communication. For example, although metadata revealing a single telephone call to a bookie may suggest that the caller is placing a bet, analysis of metadata over time could reveal that someone has a gambling problem, particularly if the call records also reveal a series of calls to payday loan services. With a database of telephony metadata reaching back five years, many of these kinds of patterns will emerge once the collected phone records are subjected to even the most basic analytic techniques. In short, aggregated telephony metadata allows the NSA to construct social graphs and to study their evolution and communications patterns over days, weeks, months, or even years. Metadata analysis can reveal the rise and fall of intimate relationships, the diagnosis of a life-threatening disease, the telltale signs of a corporate merger or acquisition, or the social dynamics of a group of associates.

7. Much information can be gathered about individuals from metadata—current programs raise significant privacy concerns

Edward W. Felten, Professor, Computer Science and Public Affairs, Princeton University, Testimony before the Senate Intelligence Committee, 10—2—13, <http://www.judiciary.senate.gov/pdf/10-2-13FeltenTestimony.pdf>, accessed 10-8-13. The work of these researchers suggests that the power of metadata analysis and its potential impact on the privacy of individuals increases with the scale of the data collected and analyzed. Just as multiple calls by the same person reveal more than a single call, so too does a database containing calling data about millions of people reveal more information about the individuals contained within it than a database with calling data about just one person. The privacy impact of collecting all communications metadata about a single person for long periods of time is qualitatively different than doing so over a period of a few days. Similarly, the privacy impact of assembling the call records of every American is vastly greater than the impact of collecting data about a single person or even groups of people. Mass collection not only allows the NSA to learn information about more people, but it also gives the NSA the ability to learn new, previously private facts about innocent Americans that it could not have learned simply by collecting the information about a few, specific individuals.

8. The programs do collect content

Thomas R. Eddlem, “The NSA Domestic Surveillance Lie,” *NEW AMERICAN*, 9—22—13, www.thenewamerican.com/usnews/politics/item/16580-the-nsa-domestic-surveillance-lie, accessed 10-13-13. On July 31, 2013, at the Black Hat USA 2013 conference, NSA Director General Keith Alexander laid out the entirety of what the NSA was supposedly collecting: I thought it would be important to give you a picture of what our analysts actually see. There it is ... as you can see, what you have is the date and time of the call, the calling number and the call — the duration of the call. And we also put in the origin of the metadata data.... This does not include the content of the communications. This does not include your phone calls or mine, your emails, nor mine, your SMS messages. There is no content. By the time Alexander said those words, they were already out of date. That same day Greenwald published in *The Guardian* information on the NSA’s XKeyscore program, a program that collects millions of e-mails from American citizens without a warrant, along with “nearly everything a user does on the Internet.” Later, other NSA programs were also revealed to have collected Americans’ e-mail messages on a massive scale. In response to being busted on this lie, the Obama administration had another fallback upon which to rest their damage-control program: Even though they are collecting all Americans’ Internet data, including the full content of e-mail messages, the data had never been misused and are subject to multiple safeguards. Of course, the Fourth Amendment to the U.S. Constitution prohibits not only warrantless “searches” by the government, it bans government “seizures” of records without both a warrant and probable cause as well.

Surveillance Undesirable: Privacy—Answers to “Minimal Intrusion”

1. The NSA actually reviews a very large portion of internet communications—they ignore torrenting/streaming traffic

James Ball, “NSA Stores Metadata of Millions of Web Users for up to a Year, Secret Files Show,” GUARDIAN, 9—30—13, <http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents>, accessed 10-2-13. However, critics were skeptical of the reassurances, because large quantities of internet data is represented by music and video sharing, or large file transfers – content which is easy to identify and dismiss without entering it into systems. Therefore, the NSA could be picking up a much larger percentage of internet traffic that contains communications and browsing activity. Journalism professor and internet commentator Jeff Jarvis noted: “[By] very rough, beer-soaked-napkin numbers, the NSA’s 1.6% of net traffic would be half of the communication on the net. That’s one helluva lot of ‘touching’.” Much of the NSA’s data collection is carried out under section 702 of the Fisa Amendments Act. This provision allows for the collection of data without individual warrants of communications, where at least one end of the conversation, or data exchange, involves a non-American located outside the US at the time of collection. The NSA is required to “minimize” the data of US persons, but is permitted to keep US communications where it is not technically possible to remove them, and also to keep and use any “inadvertently” obtained US communications if they contain intelligence material, evidence of a crime, or if they are encrypted. The Guardian has also revealed the existence of a so-called “backdoor search loophole”, a 2011 rule change that allows NSA analysts to search for the names of US citizens, under certain circumstances, in mass-data repositories collected under section 702.

2. The NSA has been collecting enormous quantities of data

Brennan Center for Justice, New York University School of Law, “Are They Allowed to Do That? A Breakdown of Selected Government Surveillance Programs,” 2013, www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf, accessed 10-12-13. Since 2006, the National Security Agency (NSA) has been secretly collecting the phone records of millions of Americans from some of the largest telecommunications providers in the United States, via a series of regularly renewed requests by the Federal Bureau of Investigation (FBI). Although the NSA is not collecting the contents of all phone calls, it is collecting records of who called whom, when and for how long. There are also reports that the NSA has been collecting similar information about e-mails, internet searches, and credit card transactions. The government has acknowledged some aspects of this collection program, but claims that officials do not actually look at the collected data in more detail without reasonable suspicion that some element of it concerns a foreign terrorist organization.

3. The NSA program will be used to create huge ‘knowledge databases’ on our everyday activities

American Civil Liberties Union, HOW THE NSA’S SURVEILLANCE PROCEDURES THREATEN AMERICANS’ PRIVACY, 2013, https://www.aclu.org/files/assets/explainer_v4.pdf, accessed 10-2-13. 7. The Procedures contemplate that the NSA will maintain “knowledge databases” containing sensitive information about Americans. To determine whether a target is a foreigner abroad, the Procedures contemplate that the NSA will consult various NSA databases containing information collected by it and other agencies through signals intelligence, human intelligence, law enforcement, and other means. These databases—referred to as “NSA content repositories” and “knowledge databases”—apparently house internet data, including metadata that reveals online activities, as well as telephone numbers and email addresses that the agency has reason to believe are being used by U.S. persons. The Procedures’ reference to “Home Location Registers,” which receive updates whenever a phone “moves into a new service area,” suggests that the NSA also collects some form of location information about millions of Americans’ cellphones. The Procedures do not say what limits apply to these databases or what safeguards, if any, are in place to protect Americans’ constitutional rights.

Surveillance Undesirable: Privacy—Answers to “Not Domestic”

1. The program covers domestic material—up to 75% of all internet traffic

REUTERS, “NSA Surveillance covers 75 Percent of U.S. Internet Traffic,” 8—20—13,

www.reuters.com/article/2013/08/21/us-usa-security-nsa-idUSBRE97K02V20130821, accessed 10-13-13.

The National Security Agency's surveillance network has the capacity to reach around 75 percent of all U.S. Internet communications in the hunt for foreign intelligence, the Wall Street Journal reported on Tuesday. Citing current and former NSA officials, the newspaper said the 75 percent coverage is more of Americans' Internet communications than officials have publicly disclosed. The Journal said the agency keeps the content of some emails sent between U.S. citizens and also filters domestic phone calls made over the Internet. The NSA's filtering, carried out with telecom companies, looks for communications that either originate or end abroad, or are entirely foreign but happen to be passing through the United States, the paper said. But officials told the Journal the system's broad reach makes it more likely that purely domestic communications will be incidentally intercepted and collected in the hunt for foreign ones. In response to a request for comment, NSA said its intelligence mission "is centered on defeating foreign adversaries who aim to harm the country. We defend the United States from such threats while fiercely working to protect the privacy rights of U.S. persons. "It's not either/or. It's both," NSA said in an email statement to Reuters. The Journal said that these surveillance programs show the NSA can track almost anything that happens online, so long as it is covered by a broad court order, the Journal said.

2. Even though it serves “foreign intelligence” interests, the program engages in domestic spying

Margot Kaminski, Executive Director, Information Society Project, Yale Law School, “PRISM’s Legal Basis: How We Got Here, and What We Can Do to Get Back,” THE ATLANTIC, 6—7—13,

www.theatlantic.com/national/archive/2013/06/prisms-legal-basis-how-we-got-here-and-what-we-can-do-to-get-back/276667/, accessed 10-13-13.

The Fourth Amendment prevents dragnet surveillance by requiring law enforcement to go to courts and show probable cause. These dual requirements of court oversight and a legitimate, targeted investigation ensure that people will not be subject to general searches by an abusive government. But intelligence-gathering that involves "the activities of foreign powers" is treated differently, whether it occurs inside or outside of the United States. Foreign intelligence is the exception that has swallowed the Fourth Amendment whole. As my colleague Anjali Dalal points out, people probably believe that foreign intelligence law is "supposed to be going after foreign intelligence," but its impact on Americans is surprisingly broad. In 1978, Congress set up a system governing foreign intelligence surveillance. The surveillance programs leaked in the past two days are the results of the post-9/11 version of this system. The Verizon call records, which include phone numbers, location data, and timestamps, were authorized as the collection of "business records" under the PATRIOT Act. And the PRISM program--which allows the NSA to access content such as emails, search histories, and audio chats-- is authorized as part of "foreign intelligence" gathering under the 2008 Amendments to the Foreign Intelligence Surveillance Act (FISA). It is crucial to understand that the foreign intelligence system as it currently exists fails to require both adequate targeting and adequate oversight. The system allows intelligence agencies to gather an enormous amount of information "incidental" to any investigations. And it does so with minimal court and Congressional oversight. If the revelations of the past two days have taught us anything, it is that revision of our foreign intelligence surveillance system is a constitutional necessity. If the Fourth Amendment is to have any meaning, Congress must untangle the current web of broad authorizations and broad secrecy that allows the government to escape judicial accountability for its acts. First, there is the question of whom the surveillance targets. PRISM spies on Americans. The Director of National Intelligence emphasized yesterday that PRISM targets only "non-U.S. persons located outside the United States." But the press release also acknowledges that "information about U.S. persons" may be "incidentally acquired" in such pursuits. Targeting is not the same as collecting; the program may "target" foreign persons, but "acquire" information on Americans.

Surveillance Undesirable: Privacy—Answers to “Not Domestic” [cont’d]

3. The administration is collecting metadata on Americans—do not believe claims to the contrary

Thomas R. Eddlem, “The NSA Domestic Surveillance Lie,” NEW AMERICAN, 9—22—13,

www.thenewamerican.com/usnews/politics/item/16580-the-nsa-domestic-surveillance-lie, accessed 10-13-13.

The Bush administration, which initiated the denials of spying on Americans, implied that any U.S. surveillance within the country was strictly limited to likely terrorists — people that courts ruled to be dangerous based on the available evidence. President Bush stated on April 20, 2004: There are such things as roving wiretaps. Now, by the way, any time you hear the United States government talking about wiretap, it requires — a wiretap requires a court order. Nothing has changed, by the way. When we’re talking about chasing down terrorists, we’re talking about getting a court order before we do so. It’s important for our fellow citizens to understand, when you think Patriot Act, constitutional guarantees are in place when it comes to doing what is necessary to protect our homeland, because we value the Constitution. On March 20 of this year, the director of national intelligence, Admiral James Clapper, also denied that there has been wholesale monitoring of Americans’ communications, when he was asked by Oregon Senator Ron Wyden, “Does the NSA collect any type of data at all on millions or hundreds of millions of Americans?” Director of National Intelligence and Admiral James Clapper: “No, sir.” Wyden: “It does not?” Clapper: “Not wittingly. There are cases where they could inadvertently perhaps collect, but not wittingly.” Oops. We meant to say we are collecting metadata on Americans. Both administrations engaged in flat-out lies to the American people, but the Obama administration has been caught in lie after lie as it continually retreats from its official story. Both administrations engaged in flat-out lies to the American people, but the Obama administration has been caught in lie after lie as it continually retreats from its official story. The official story changed dramatically with Snowden’s whistleblowing. Snowden told Greenwald back on June 9, 2013 that the NSA — once devoted to foreign intelligence — was increasingly focused upon surveilling Americans. “The NSA specifically targets the communications of everyone. It ingests them by default. It collects them in its system and it filters them and it analyzes them and it measures them and it stores them for a period of time.” It had gone so far, the former Booz-Allen-Hamilton employee claimed, “I, sitting at my desk, certainly had the authority to wiretap anyone, from you or your accountant, to a federal judge or even the president, if I had a personal email.” Though Obama administration officials denied Snowden’s sweeping charges (Snowden was later validated), they had to backtrack after Greenwald published information on the NSA’s collection of Americans’ Internet “meta-data” under the agency’s PRISM program. James Clapper retracted his statement to Wyden on June 9 during NBC’s Sunday Today show: I responded in what I thought was the most truthful, or least untruthful manner by saying no. And again, to go back to my metaphor. What I was thinking of is looking at the Dewey Decimal numbers — of those books in that metaphorical library — to me, collection of U.S. persons’ data would mean taking the book off the shelf and opening it up and reading it.

Surveillance Undesirable: Privacy—Answers to “Oversight—FISA Court”

1. The FISA Court does not act as a check on surveillance—multiple reasons

Laura K. Donohue, Professor, Law, Georgetown University, Testimony before the Senate Judiciary Committee, 10—2—13, <http://www.judiciary.senate.gov/pdf/10-2-13DonohueTestimony.pdf>, accessed 10-8-13.

In at least three important ways, the Foreign Intelligence Surveillance Court no longer serves the purpose for which it was designed. First, it was created to determine whether sufficient evidence existed to target individuals within the United States, prior to the collection of such information. But the Court has abdicated this responsibility to the executive branch generally, and to the NSA in particular. Continued noncompliance underscores concern about relying on the intelligence community to protect the Fourth Amendment rights of U.S. persons. Second, Congress did not envision a law-making role for the Court. Its decisions were not to serve as precedent, nor was the Court to offer lengthy legal analyses, crafting in the process, for instance, exceptions to the Fourth Amendment warrant requirement or defenses of wholesale surveillance programs. Third, instead of being a neutral, disinterested magistrate, the court has become highly politicized and appears to have failed to act as an effective check on the exercise of surveillance authorities. The manner of appointment of judges to the court, lack of technical expertise, and absence of an effective adversarial process has here harmed the Court’s ability to function.

2. The Court fails—the NSA ignores it

Laura K. Donohue, Professor, Law, Georgetown University, Testimony before the Senate Judiciary Committee, 10—2—13, <http://www.judiciary.senate.gov/pdf/10-2-13DonohueTestimony.pdf>, accessed 10-8-13.

FISC’s primary order authorizing the collection of telephony metadata required that designated NSA officials make a finding that there is “reasonable, articulable suspicion” (“RAS”) that a seed identifier proposed for query is associated with a particular foreign terrorist organization prior to its use. Documents recently released as a result of court orders in a related FOIA case establish that for nearly three years, the NSA did not follow these procedures—despite the fact that numerous officials at the agency were aware of the violation. Noncompliance incidents have continued. Collectively, these incidents raise serious question as to whether FISC is performing the functions it was designed to address.

3. The programs violate the Fourth Amendment, even if signed off on by a FISA judge

Elizabeth Goitein, co-director, Liberty and National Security Program, Brennan Center for Justice, New York University School of Law, “The Danger of American Apathy on NSA Surveillance,” CHRISTIAN SCIENCE MONITOR, 7—31—13, www.csmonitor.com/Commentary/Opinion/2013/0731/The-danger-of-American-apathy-on-NSA-surveillance, accessed 10-13-13.

The most obvious answer is that these programs may be illegal. The government admits it obtains Americans’ telephone records in bulk, but claims officials do not examine them unless there is reason to suspect a terrorist link. Section 215 of the Patriot Act, however, requires the government to establish a record’s investigative relevance before obtaining it – not after. The PRISM program, which collects information from Internet service providers, is ostensibly legal because it “targets” foreigners. But the program tolerates extensive “inadvertent” and “incidental” collection of Americans’ information – including information the government needs a warrant to obtain under the Fourth Amendment. Yes, a secret court approved these programs. That should not start and end the discussion about their legality. Judges make mistakes, and – as recent reporting on the secret Foreign Intelligence Service Act (FISA) Court has underscored – they are far more likely to do so when they hear only the facts and arguments that one side chooses to present. When citizens have gone to the regular courts to challenge government surveillance, the government has successfully argued that the courts cannot even consider their claims. The programs also threaten Americans’ privacy. It is disingenuous for officials to characterize the “metadata” being collected as mere phone numbers. Sophisticated computer programs can glean volumes of sensitive information from this metadata about people’s relationships, activities, and even beliefs. The government knows very well how revealing call records can be; that is why it considers the program so valuable.

Surveillance Undesirable: Privacy—Answers to “Oversight—FISA Court” [cont’d]

4. The FISA Court does not provide meaningful oversight—does not even understand the technologies

Laura K. Donohue, Professor, Law, Georgetown University, Testimony before the Senate Judiciary Committee, 10—2—13, <http://www.judiciary.senate.gov/pdf/10-2-13DonohueTestimony.pdf>, accessed 10-8-13.

A critical part of FISC’s failure to provide effective oversight of the process relates to the Court’s decision to have the NSA perform the targeting decision. Part of the problem also stems from the court’s discomfort with the technological aspects of the collection and analysis of digital information. For much of the discussion of noncompliance incidents, for instance, it appears that neither the NSA nor FISC has an adequate understanding of how the algorithms operate. Neither did they understand the type of information that had been incorporated into different databases, and whether they had been subjected to the appropriate legal analysis prior to data mining. A similar problem may accompany the reporting requirements to Congress. In March 2009, for example, the Department of Justice had submitted several FISC opinions and Government filings relating to the discovery and remediation of compliance incidents in its handling of bulk telephony metadata to the Chairmen of the Intelligence and Judiciary Committees. A subsequent letter noted that the House and Senate Intelligence and Judiciary Committees had received briefings in March, April, and August, before receiving a copy of the NSA’s review in September 2009. To the extent that the representations of the agency are heavily dependent on technical knowledge, the implications may not be readily transparent to lawmaker.

5. The FISA Court fails—too politicized

Laura K. Donohue, Professor, Law, Georgetown University, Testimony before the Senate Judiciary Committee, 10—2—13, <http://www.judiciary.senate.gov/pdf/10-2-13DonohueTestimony.pdf>, accessed 10-8-13.

Congress tried to avoid the politicization of the Foreign Intelligence Surveillance Court by requiring that (a) the eleven judges be selected by the Chief Justice of the Supreme Court from at least seven different federal districts; (b) the judges serve staggered terms of up to seven years; and (c) having once served, such judges are ineligible for further service. To ensure further diversity, any federal district court judge (including a senior judge), who has not previously served on FISC, may be selected. The Foreign Intelligence Surveillance Court of Review, in turn, is comprised of judges selected by the Chief Justice. The problem with this system is that it has failed. To the extent that political ideology reflects in the appointments process, the court can only be viewed as highly politicized. The past two Chief Justices have been appointed by Republican presidents, and their selections for the Foreign Intelligence Surveillance Court and Court of Review have been heavily weighted towards judges that have been nominated by Republican Administrations. (See Fig. 1) Only one of the current eleven judges serving on FISC is a Democratic nominee. Over the past decade, of the 20 judges appointed to FISC and FISCR, only three were democratic nominees to the bench. At least two of the nominees to the court over the past decade, moreover, have rejected FISA as being an unconstitutional intrusion on the President’s inherent authorities. Laurence Silberman, from the DC Circuit, testified to Congress in 1978 (when FISA was being debated) that the legislation violated the U.S. Constitution. Silberman, who had previously served as Deputy Attorney General, was “absolutely convinced that the administration bill, if passed, would be an enormous and fundamental mistake which the congress and the American people would have reason to regret.” For Silberman, the judiciary’s role in any national security electronic surveillance should be circumscribed. He explained, I find the notion that the President’s constitutional authority to conduct foreign affairs and to command the armed forces precludes congressional intervention into the manner by which the executive branch gathers intelligence, by electronic or other means, to be unpersuasive, and in that respect I agree with my colleague here to the left. But to concede the propriety of a congressional role in this matter is by no means—and this is the burden of my testimony—to concede the propriety or constitutionality of the judicial role created by the administration’s bill. The chief concern was not a so-called “imperial Presidency”, but the advent of an imperial judiciary. The authorities thus transferred to the Foreign Intelligence Surveillance Court represented an unconstitutional erosion of executive power. In addition to Silberman, Ralph Guy, a 6th Circuit judge, as a U.S. attorney, argued for the government in *U.S. v. U.S. District Court*, that the president did not need any type of a warrant to engage in national security surveillance.

Surveillance Undesirable: Privacy—Answers to “Oversight—FISA Court” [cont’d]

6. The FISA Court fails—acts as a rubber stamp

Laura K. Donohue, Professor, Law, Georgetown University, Testimony before the Senate Judiciary Committee, 10—2—13, <http://www.judiciary.senate.gov/pdf/10-2-13DonohueTestimony.pdf>, accessed 10-8-13.

Augmenting the politicization of FISC and FISCER is the rather remarkable success rate enjoyed by the government in its applications to the court. Scholars have noted that it is “unparalleled in any other American court.” Much attention has been paid in this regard to the almost nonexistent rate of denial of orders under the electronic communications intercept authorities. Almost no attention, however, has been paid to business records and the production of tangible goods under 50 U.S.C. §1862(c)(2)—the section most relevant to the metadata programs. Consistent with the restrictions, it appears that FISC has never denied an application for an order under this section. That is, of 751 applications since 2005, all 751 have been granted. (See Fig. 2) These numbers are remarkable not least because any one order, as we have seen with the telephony metadata program, could result in the collection of millions of records on millions of U.S. persons. In light of the utter lack of adversarial counsel in in camera, ex parte proceedings, these numbers at least raise serious question about the extent to which FISC and FISCER perform the function they were envisioned to serve

7. FISA does not check the NSA—the agency pushes the envelope and the judges on the court refuse to curtail the agency’s activities

Scott Lemieux, Assistant Professor, Political Science, College of Saint Rose, “The NSA Can’t Be Trusted,” AMERICAN PROSPECT, 8—19—13, <http://prospect.org/article/nsa-cant-be-trusted>, accessed 10-8-13.

There’s some truth to this, but this violation still raises some serious questions. It seems likely that the FISA court—which thanks to the unwise decision by Congress to confer the unilateral power to select FISA judges to the Chief Justice of the Supreme Court is dominated by conservative Republicans—is permitting the NSA to use techniques of questionable legality. The audit makes clear that the NSA is determined to push the legal envelope, and it’s hard to view the FISA court as a reliable check on potential abuses. Indeed, the chief judge of the FISA court has said that his tribunal “does not have the capacity to investigate issues of noncompliance.” The leaked audit makes President Obama’s reassurances about the NSA’s surveillance regime ring hollower than ever. Above all, it compellingly shows the need for greater congressional oversight. It’s never easy to be optimistic about Congress stepping up, but this important story will hopefully be a nudge in the right direction.

8. Oversight is minimal—the FISA court approves most requests and the court cannot oversee compliance

Brennan Center for Justice, New York University School of Law, “Are They Allowed to Do That? A Breakdown of Selected Government Surveillance Programs,” 2013,

www.brennancenter.org/sites/default/files/analysis/Government%20Surveillance%20Factsheet.pdf, accessed 10-12-13.

To collect the kind of phone records it did from Verizon, the government must obtain a Section 215 order from the Foreign Intelligence Surveillance Court (FISA court) — a federal court established under FISA which oversees government applications to conduct surveillance for the purposes of obtaining foreign intelligence. The request for the order, and the court’s ruling, are classified. The number of Section 215 orders has soared in recent years, from just 21 applications in 2009 to 212 applications in 2012. None of the applications in 2012 were denied by the FISA court. Classified reports about these applications are submitted to Congress’s intelligence and judiciary committees. Unclassified aggregate numbers, such as the above, are sent to Congress annually. When it comes to Section 702, the law cited for PRISM, the FISA court’s role is more limited. Even though Section 702 does not allow the intentional surveillance of U.S. persons, the government is not required to go before the court to obtain individual surveillance orders. Instead, the court approves the “targeting” and “minimization” procedures described above to limit the amount of information about law-abiding Americans that is intercepted, retained, and disseminated. In deciding whether to approve the procedures, the court reviews whether they are consistent with the Fourth Amendment to the Constitution. But it has no ongoing authority to determine if the government is complying with these procedures, and both the procedures and the court orders relating to them are classified. Some information about Section 702 programs must be reported to Congress’s intelligence and judiciary committees, including significant legal opinions of the FISA court. However, these reports are generally classified and not shared.

Surveillance Undesirable: Privacy—Answers to “Oversight—FISA Court” [cont’d]

9. The existence of the programs and their broad scope proves that FISA court oversight fails

Margot Kaminski, Executive Director, Information Society Project, Yale Law School, “PRISM’s Legal Basis: How We Got Here, and What We Can Do to Get Back,” THE ATLANTIC, 6—7—13, www.theatlantic.com/national/archive/2013/06/prisms-legal-basis-how-we-got-here-and-what-we-can-do-to-get-back/276667/, accessed 10-13-13.

At the core of the problem is that the Foreign Intelligence Surveillance Court (FISA Court), which meets in secret and does not publish its opinions, itself does not provide adequate oversight. When Congress changed the standard for targeting foreign individuals in 2008, it abolished the ability of the FISA Court to evaluate whether the government had any real cause to target an individual or group of individuals. The Supreme Court itself disputes whether the FISA Court enforces the Fourth Amendment. The “minimization procedures” touted by the Director of National Intelligence as adequate privacy safeguards are established by the government, evaluated by the government, and are subject to review by a secret court—if review occurs at all. And as a general practice, FISA “minimization” has not been true minimization: it occurs after information is already acquired. The existence of PRISM and the Verizon metadata program, both authorized by the FISA Court, confirms that a secret court broadly authorized by an uninformed Congress will not adequately protect the Fourth and First Amendment rights of American citizens on American soil.

10. The FISA court has authorized the NSA to monitor every single phone call

Alex Abdo, Staff Attorney, ACLU National Security Project, “Latest FISA Court Opinion: A Preview of Surveillance without Limits,” FREE FUTURE, American Civil Liberties Union, 9—18—13, <https://www.aclu.org/blog/national-security/latest-fisa-court-opinion-preview-surveillance-without-limits>, accessed 10-8-13.

The secret Foreign Intelligence Surveillance Court (FISC) released an opinion yesterday explaining its decision to allow the NSA to collect a record of every single phone call made by every single American every single day. The program—which we have called the “mass call-tracking program” in our lawsuit challenging it—is one of the most sweeping surveillance programs ever approved by a court or instituted in a democracy. And so you might reasonably expect that a judicial justification of the program would require a lengthy opinion explaining in detail how such indiscriminate surveillance can possibly be lawful. Not so—the FISC managed to approve the indefinite tracking of every American’s phone calls in under 30 pages.

11. Amendments and reforms have been a failure—the surveillance is not subjected to meaningful judicial oversight

American Civil Liberties Union, “United States’ Compliance with the International Covenant on Civil and Political Rights,” SHADOW REPORT TO THE FOURTH PERIODIC REPORT OF THE UNITED STATES, 9—13—13, p. 49-50.

The U.S. government’s responses to the Committee state that amendments to the FISA have “enhance[d] judicial and Congressional oversight” by giving the FISC a “continuing and active role in overseeing certain NSA collection activities.” But those answers belie the weakness of the current surveillance-oversight scheme. Until Congress enacted section 702 as part of the FISA Amendments Act (FAA), in 2008, the FISA generally prohibited the government from conducting electronic surveillance without first obtaining an individualized and particularized order from the FISC. In order to obtain a court order, the government was required to show that there was probable cause to believe that its surveillance target was an agent of a foreign power, such as a foreign government or terrorist group. It was also generally required to identify the facilities to be monitored. Section 702, in contrast, has as its defining feature the lack of ongoing judicial oversight. The FISC does not review individualized surveillance applications. Nor does it have the right to ask the government why it is initiating any particular surveillance program. Instead, the FISC’s role is limited to reviewing the government’s targeting and minimization procedures. And even with respect to those procedures, the FISC’s role is to review the procedures at the outset of any new surveillance program; it does not have the authority to supervise the implementation of those procedures over time. Section 702 allows the U.S. government to conduct electronic surveillance without indicating to the FISC whom it intends to target or which facilities, telephone lines, email addresses, places, premises, or property at which its surveillance will be directed. Further, the law does not require the government to make any showing to the court—or even make an internal executive determination—that the target is a foreign agent or engaged in terrorism. The target could be a human rights activist, a media organization, a geographic region, or even an entire country. And because section 702 does not require the government to identify the specific targets and facilities to be surveilled, it permits the acquisition of these communications en masse. A single acquisition order may be used to justify the surveillance of communications implicating thousands or even millions of people, for a year at a time.

Surveillance Undesirable: Privacy—Answers to “Oversight—General”

1. Oversight isn’t working now—secrecy, weak FISA court

Jameel Jaffer, Deputy Legal Director, ACLU Foundation and Laura W. Murphy, Director, Washington Legislative Office, ACLU, Testimony before the House Judiciary Committee, 7—17—13, <http://judiciary.house.gov/hearings/113th/07172013/Jaffer%2007172913.pdf>, accessed 10-2-13.

Over the last six weeks it has become clear that the National Security Agency (NSA) is engaged in far-reaching, intrusive, and unlawful surveillance of Americans’ telephone calls and electronic communications. That the NSA is engaged in this surveillance is the result of many factors. The Foreign Intelligence Surveillance Act (FISA) affords the government sweeping power to monitor the communications of innocent people. Excessive secrecy has made congressional oversight difficult and public oversight impossible. Intelligence officials have repeatedly misled the public, Congress, and the courts about the nature and scope of the government’s surveillance activities. Structural features of the Foreign Intelligence Surveillance Court (FISC) have prevented that court from serving as an effective guardian of individual rights. And the ordinary federal courts have improperly used procedural doctrines to place the NSA’s activities beyond the reach of the Constitution.

2. Congressional oversight is ineffective—secrecy

Margot Kaminski, Executive Director, Information Society Project, Yale Law School, “PRISM’s Legal Basis: How We Got Here, and What We Can Do to Get Back,” THE ATLANTIC, 6—7—13, www.theatlantic.com/national/archive/2013/06/prisms-legal-basis-how-we-got-here-and-what-we-can-do-to-get-back/276667/, accessed 10-13-13.

This brings us to the issue of oversight: who is watching the watchers? The Director of National Intelligence assures us that PRISM is “subject to oversight by the Foreign Intelligence Surveillance Court, the Executive Branch, and Congress.” It is true that in December 2012 Congress renewed the law that allows PRISM to exist. But what kind of oversight did Congress actually provide? When Senators Ron Wyden and Mark Udall asked whether communications by Americans had been gathered under the law, the Director of National Intelligence responded that it was not possible to identify the number of people in the United States whose communications were reviewed. How effective can Congressional oversight be if Congress does not understand the scope and nature of the programs it has authorized?

3. The oversight framework is frequently gamed

John Prados, senior fellow, National Security Archive, “Demystifying the NSA Surveillance Program,” HISTORY NEWS NETWORK, 7—15—13, <http://hnn.us/article/152605>, accessed 10-13-13.

The Surveillance is properly accountable because all three branches of government approved it. This argument is false. Only the Executive branch conceived and approved the NSA surveillance. Not only was it conducted for several years without reference to the FISC, which had the statutory authority to review all applications for such surveillance, the Executive merely briefed Congress on the surveillance. Notification does not equate to approval. The degree of congressional involvement that the Executive accorded did not permit oversight in any meaningful way. The Executive then went to Congress late in the second Bush administration and obtained amendments to the Patriot and Foreign Surveillance Acts, providing misleading justifications and then immediately interpreting its powers expansively. Only under that rubric did the Executive approach the FISC where it obtained a legal review that was again given a maximalist interpretation. The existing framework for congressional oversight and legal review was gamed, intelligence officials misled and outright lied before Congress, and the Executive now argues that participation by the three branches of government establishes a solid base of legality.

Surveillance Undesirable: Privacy—Answers to “Oversight—General” [cont’d]

4. The NSA has repeatedly violated the law in its surveillance activities

Patrick Leahy, U. S. Senator, Testimony before the Senate Judiciary Committee, 10—2—13, lexis.

As we continue to re-examine the intelligence community's use of FISA authorities, let's be clear that no one underestimates the threats that our country continues to face, or the difficulty of identifying and meeting those threats. We can all agree that we should equip the intelligence community with the necessary and appropriate tools to help keep us safe. But I hope that we can also agree that there have to be limits on the surveillance powers we give to the government. Just because something is technologically possible, and just because something may be deemed technically legal, does not mean that it is the right thing to do. This summer, many Americans learned for the first time that Section 215 of the USA PATRIOT Act has for years been secretly interpreted to authorize the collection of Americans' phone records on an unprecedented scale. The American public also learned more about the government's collection of internet content data through the use of Section 702 of FISA. Since the Committee's last hearing on these revelations in late July, the American people have learned a great deal more. They have learned that the NSA has engaged in repeated, substantial legal violations in its implementation of both Section 215 and Section 702 of FISA. For example, the NSA collected, without a warrant, the content of tens of thousands of wholly domestic emails of innocent Americans. The NSA also violated a FISA Court order by regularly searching the Section 215 phone records database without meeting the standard imposed by the Court.

5. FISA is supposed to significantly restrict the NSAs domestic surveillance capabilities

Laura K. Donohue, Professor, Law, Georgetown University, Testimony before the Senate Judiciary Committee, 10—2—13, <http://www.judiciary.senate.gov/pdf/10-2-13DonohueTestimony.pdf>, accessed 10-8-13.

Congress purposefully circumscribed the NSA's authorities in the Foreign Intelligence Surveillance Act by adopting four key protections. First, any information obtained from an electronic intercept had to be tied to a specific person or entity, identified as a foreign power or an agent thereof, prior to the collection of the information. Second, the government had to demonstrate probable cause that the target, about whom information was to be collected, was a foreign power or an agent thereof. For U.S. persons, such probable cause could not be established solely on the basis of otherwise protected First Amendment activities, thus providing American citizens with a higher level of protection. Third, Congress adopted minimization procedures to restrict the type of information that could be obtained and retained. Fourth, FISA made provision for a Foreign Intelligence Surveillance Court (“FISC”) to oversee the process. Designed to introduce a neutral, disinterested magistrate into the equation, FISC's role was, narrowly, to ascertain whether the government had met the appropriate requirements for targeting prior to the acquisition of information. All of these limits dealt, specifically, with electronic communications. Over time, the statute expanded to apply a similar approach to physical searches, the placement of pen registers and trap and trace, and business records—as well as tangible goods.

Surveillance Undesirable: Privacy—Answers to “Social Networks Exempted”

1. NSA is using its programs to track social connections of Americans

James Risen and Laura Poitras, “N.S.A. Gathers Data on Social Connections of U.S. Citizens,” NEW YORK TIMES, 9—28—13, <http://www.nytimes.com/2013/09/29/us/nsa-examines-social-networks-of-us-citizens.html>, accessed 10-2-13.

Since 2010, the National Security Agency has been exploiting its huge collections of data to create sophisticated graphs of some Americans’ social connections that can identify their associates, their locations at certain times, their traveling companions and other personal information, according to newly disclosed documents and interviews with officials. The spy agency began allowing the analysis of phone call and e-mail logs in November 2010 to examine Americans’ networks of associations for foreign intelligence purposes after N.S.A. officials lifted restrictions on the practice, according to documents provided by Edward J. Snowden, the former N.S.A. contractor. The policy shift was intended to help the agency “discover and track” connections between intelligence targets overseas and people in the United States, according to an N.S.A. memorandum from January 2011. The agency was authorized to conduct “large-scale graph analysis on very large sets of communications metadata without having to check foreignness” of every e-mail address, phone number or other identifier, the document said. Because of concerns about infringing on the privacy of American citizens, the computer analysis of such data had previously been permitted only for foreigners. The agency can augment the communications data with material from public, commercial and other sources, including bank codes, insurance information, Facebook profiles, passenger manifests, voter registration rolls and GPS location information, as well as property records and unspecified tax data, according to the documents. They do not indicate any restrictions on the use of such “enrichment” data, and several former senior Obama administration officials said the agency drew on it for both Americans and foreigners. N.S.A. officials declined to say how many Americans have been caught up in the effort, including people involved in no wrongdoing. The documents do not describe what has resulted from the scrutiny, which links phone numbers and e-mails in a “contact chain” tied directly or indirectly to a person or organization overseas that is of foreign intelligence interest. The new disclosures add to the growing body of knowledge in recent months about the N.S.A.’s access to and use of private information concerning Americans, prompting lawmakers in Washington to call for reining in the agency and President Obama to order an examination of its surveillance policies. Almost everything about the agency’s operations is hidden, and the decision to revise the limits concerning Americans was made in secret, without review by the nation’s intelligence court or any public debate. As far back as 2006, a Justice Department memo warned of the potential for the “misuse” of such information without adequate safeguards.

2. NSA program metadata covers social connections for millions of Americans

James Ball, “NSA Stores Metadata of Millions of Web Users for up to a Year, Secret Files Show,” GUARDIAN, 9—30—13, <http://www.theguardian.com/world/2013/sep/30/nsa-americans-metadata-year-documents>, accessed 10-2-13.

The National Security Agency is storing the online metadata of millions of internet users for up to a year, regardless of whether or not they are persons of interest to the agency, top secret documents reveal. Metadata provides a record of almost anything a user does online, from browsing history – such as map searches and websites visited – to account details, email activity, and even some account passwords. This can be used to build a detailed picture of an individual's life. The Obama administration has repeatedly stated that the NSA keeps only the content of messages and communications of people it is intentionally targeting – but internal documents reveal the agency retains vast amounts of metadata. An introductory guide to digital network intelligence for NSA field agents, included in documents disclosed by former contractor Edward Snowden, describes the agency's metadata repository, codenamed Marina. Any computer metadata picked up by NSA collection systems is routed to the Marina database, the guide explains. Phone metadata is sent to a separate system. “The Marina metadata application tracks a user's browser experience, gathers contact information/content and develops summaries of target,” the analysts' guide explains. “This tool offers the ability to export the data in a variety of formats, as well as create various charts to assist in pattern-of-life development.” The guide goes on to explain Marina's unique capability: “Of the more distinguishing features, Marina has the ability to look back on the last 365 days' worth of DNI metadata seen by the Sigint collection system, regardless whether or not it was tasked for collection.” [Emphasis in original.] On Saturday, the New York Times reported that the NSA was using its metadata troves to build profiles of US citizens' social connections, associations and in some cases location, augmenting the material the agency collects with additional information bought in from the commercial sector, which is not subject to the same legal restrictions as other data. The ability to look back on a full year's history for any individual whose data was collected – either deliberately or incidentally – offers the NSA the potential to find information on people who have later become targets. But it relies on storing the personal data of large numbers of internet users who are not, and never will be, of interest to the US intelligence community. Marina aggregates NSA metadata from an array of sources, some targeted, others on a large scale. Programs such as Prism – which operates through legally compelled “partnerships” with major internet companies – allow the NSA to obtain content and metadata on thousands of targets without individual warrants.

Surveillance Undesirable: Answers to “Terrorism”—Topshelf

1. There is little credible evidence that the NSA itself has been successful in foiling attacks—other means have been used

Teun van Dongen, “The NSA Isn’t Foiling Terrorist Plots,” FOREIGN POLICY IN FOCUS, 10—9—13, www.alternet.org/nsa-isnt-foiling-terrorist-plots, accessed 10-10-13.

Admittedly we do not know how all terrorist plots have been detected. But going by what we do know, the conclusion is simple: terrorist plots have been foiled in all sorts of ways, few of which had anything to do with mass digital surveillance. True, in the case of the dismantlement of the Sauerland Cell in Germany in 2007, NSA information played a role. But whether the authorities got this information from “digital dragnet surveillance” or from more individualized and targeted monitoring is hard to tell. It might be tempting to give the NSA the benefit of the doubt, given that the organization speaks on the basis of information that we do not have. But such dubious claims about the effectiveness of the digital surveillance programs fit seamlessly into a pattern of misinformation and deceit. The U.S. government acknowledged the existence of PRISM only after Edward Snowden had leaked details about it to The Guardian. Moreover, when the news broke, President Obama and Director of National Intelligence James Clapper tried to downplay the scale of the digital data gathering, even though we know now that the NSA is essentially making a back-up of pretty much all conceivable forms of online communication. President Obama further promised that “nobody is listening to your phone calls,” but it later became clear that the NSA can access the content of phone calls and e-mails if it so desires. Congressional oversight is poor, privacy rules are frequently broken, and the NSA liberally shares data with other intelligence agencies and foreign governments. Against this background of disputed or outright false government claims, the public is wise to be skeptical of the NSA’s claims about the effectiveness of the digital surveillance programs. The recent revelations may be mind-boggling in their technological, legal, and procedural complexities, but the bottom line is quite simple: The first credible piece of evidence that these programs are doing any good in the fight against terrorism has yet to surface. Until such evidence is provided, the Obama administration is only eroding the trust of the citizens it is claiming to protect.

2. The NSA program will not catch terror groups—their activities occur on parts of the internet that resist section 702 surveillance techniques

Leonid Bershidsky, “U.S. Surveillance Is not Aimed at Terrorists,” BLOOMBERG, 6—23—13, www.bloomberg.com/news/2013-06-23/u-s-surveillance-is-not-aimed-at-terrorists.html, accessed 10-2-13.

The Netherlands’ security service, which couldn’t find recent data on the size of the Undernet, cited a 2003 study from the University of California at Berkeley as the “latest available scientific assessment.” The study found that just 0.2 percent of the Internet could be searched. The rest remained inscrutable and has probably grown since. In 2010, Google Inc. said it had indexed just 0.004 percent of the information on the Internet. Websites aimed at attracting traffic do their best to get noticed, paying to tailor their content to the real or perceived requirements of search engines such as Google. Terrorists have no such ambitions. They prefer to lurk in the dark recesses of the Undernet. “People who radicalise under the influence of jihadist websites often go through a number of stages,” the Dutch report said. “Their virtual activities increasingly shift to the invisible Web, their security awareness increases and their activities become more conspiratorial.” Radicals who initially stand out on the “surface” Web quickly meet people, online or offline, who drag them deeper into the Web underground. “For many, finally finding the jihadist core forums feels like a warm bath after their virtual wanderings,” the report said. When information filters to the surface Web from the core forums, it’s often by accident. Organizations such as al-Qaeda use the forums to distribute propaganda videos, which careless participants or their friends might post on social networks or YouTube. Communication on the core forums is often encrypted. In 2012, a French court found nuclear physicist Adlene Hicheur guilty of, among other things, conspiring to commit an act of terror for distributing and using software called Asrar al-Mujahideen, or Mujahideen Secrets. The program employed various cutting-edge encryption methods, including variable stealth ciphers and RSA 2,048-bit keys. The NSA’s Prism, according to a classified PowerPoint presentation published by the Guardian, provides access to the systems of Microsoft Corp. (and therefore Skype), Facebook Inc., Google, Apple Inc. and other U.S. Internet giants. Either these companies have provided “master keys” to decrypt their traffic -- which they deny -- or the NSA has somehow found other means. Traditional Means Even complete access to these servers brings U.S. authorities no closer to the core forums. These must be infiltrated by more traditional intelligence means, such as using agents posing as jihadists or by informants within terrorist organizations. Similarly, monitoring phone calls is hardly the way to catch terrorists. They’re generally not dumb enough to use Verizon. Granted, Russia’s special services managed to kill Chechen separatist leader Dzhokhar Dudayev with a missile that homed in on his satellite-phone signal. That was in 1996. Modern-day terrorists are generally more aware of the available technology. At best, the recent revelations concerning Prism and telephone surveillance might deter potential recruits to terrorist causes from using the most visible parts of the Internet. Beyond that, the government’s efforts are much more dangerous to civil liberties than they are to al-Qaeda and other organizations like it.

Surveillance Undesirable: Answers to “Terrorism”—Biological

1. Bioweapons make lousy terror weapons—difficult to disperse, subject to countermeasures, too hard to do

John Mueller, Professor, Political Science, Ohio State University, *OVERBLOWN: HOW POLITICIANS AND THE TERRORISM INDUSTRY INFLATE NATIONAL SECURITY THREATS, AND WHY WE BELIEVE THEM*, 2009, p. 21-22.

For the most destructive results, biological weapons need to be dispersed in very low-altitude aerosol clouds. Because aerosols do not appreciably settle, pathogens like anthrax (which is not easy to spread or catch and is not contagious) would probably have to be sprayed near nose level. Moreover, 90 percent of the microorganisms are likely to die during the process of aerosolization, and their effectiveness could be reduced still further by sunlight, smog, humidity, and temperature changes. Explosive methods of dispersion may destroy the organisms, and, except for anthrax spores, long-term storage of lethal organisms in bombs or warheads is difficult: even if refrigerated, most of the organisms have a limited lifetime. The effects of such weapons can take days or weeks to have full effect, during which time they can be countered with medical and civil defense measures. And their impact is very difficult to predict; in combat situations they may spread back onto the attacker. In the judgment of two careful analysts, delivering microbes and toxins over a wide area in the form most suitable for inflicting mass casualties—as an aerosol that can be inhaled—requires a delivery system whose development "would outstrip the technical capabilities of all but the most sophisticated terrorist." Even then effective dispersal could easily be disrupted by unfavorable environmental and meteorological conditions." After assessing, and stressing, the difficulties a nonstate entity would find in obtaining, handling, growing, storing, processing, and dispersing lethal pathogens effectively, biological weapons expert Milton Leites compares his conclusions with glib pronouncements in the press about how biological attacks can be pulled off by anyone with "a little training and a few glass jars," or how it would be "about as difficult as producing beer." He sardonically concludes, "The less the commentator seems to know about biological warfare the easier he seems to think the task is."

2. Bioterror threat is exaggerated--few groups have attempted it, significant tech/delivery barriers

Gregory D. Koblenz, Assistant Professor, Department of Public and International Affairs and Deputy Director, Biodefense Program, George Mason University, "Biosecurity Reconsidered," *INTERNATIONAL SECURITY*, Spring 2010, p. 96+, ASP. The threat of bioterrorism, however, may not be as severe as some have portrayed it to be. Few terrorist groups have attempted to develop a biological weapons capability, and even fewer have succeeded. Prior to the anthrax letter attacks in 2001, only one group, the disciples of guru Bhagwan Shree Rajneesh in Oregon, managed to cause any casualties with a biological agent. 86 The U.S. intelligence community estimates that of the fifteen terrorist groups that have expressed an interest in acquiring biological weapons, only three have demonstrated a commitment to acquiring the capability to cause mass casualties with these weapons. 87 Groups such as Japan's Aum Shinrikyo and al-Qaida have demonstrated the desire to cause mass casualties and an interest in using disease as a weapon. Despite concerted efforts by both groups to produce deadly pathogens and toxins, however, neither has caused any casualties with such weapons, let alone developed a weapon capable of causing mass casualties. The failures experienced by these groups illustrate the significant hurdles that terrorists face in progressing beyond crude weapons suitable for assassination and the contamination of food supplies to biological weapons based on aerosol dissemination technology that are capable of causing mass casualties. 88

3. Bioweapons use is unlikely—very difficult to deploy and control

John Mueller, Professor, Political Science, Ohio State University, *OVERBLOWN: HOW POLITICIANS AND THE TERRORISM INDUSTRY INFLATE NATIONAL SECURITY THREATS, AND WHY WE BELIEVE THEM*, 2009, p. 20-21.

Properly developed and deployed, biological weapons could indeed, it thus far only in theory, kill hundreds of thousands, perhaps even millions of people. The discussion remains theoretical because biological weapons have scarcely ever been used. Belligerents have eschewed such weapons with good reason: they are extremely difficult to deploy and to control. Terrorist groups or rogue states may be able to solve such problems in the future with advances in technology and knowledge, but, notes scientist Russell Seitz, while bioterrorism may look easy on paper, "the learning curve is lethally steep in practice." The record so far is unlikely to be very encouraging. For example, Japan reportedly infected wells in Manchuria and bombed several Chinese cities with plague-infested fleas before and during World War II. These ventures (by a state, not a terrorist group) may have killed thousands of Chinese, but they apparently also caused considerable unintended casualties among Japanese troops and seem to have had little military impact.

Surveillance Undesirable: Answers to “Terrorism”—Effectiveness Exaggerated

1. The program has only stopped one attack—should be ended

Yochai Benkler, “Fact: The NSA Gets Negligible Intel from Americans’ Metadata. So End Collection,” GUARDIAN, 10—8—13, <http://www.theguardian.com/commentisfree/2013/oct/08/nsa-bulk-metadata-surveillance-intelligence>, accessed 10-10-13. Congress may be on the verge of prohibiting the NSA from continuing its bulk telephony metadata collection program. Two weeks ago, the Senate national security dissenters: Wyden, Udall, Paul, and Blumenthal proposed prohibition. Last week, the move received a major boost from a bipartisan proposal by core establishment figures: Senator Patrick Leahy, and Representatives Jim Sensenbrenner and John Conyers. It's a prohibition whose time has come. Dragnet surveillance, or bulk collection, goes to the heart of what is wrong with the turn the NSA has taken since 2001. It implements a perpetual "state of emergency" mentality that inverts the basic model outlined by the fourth amendment: that there are vast domains of private action about which the state should remain ignorant unless it provides clear prior justification. And all public evidence suggests that, from its inception in 2001 to this day, bulk collection has never made more than a marginal contribution to securing Americans from terrorism, despite its costs. In a 2 October hearing of the Senate judiciary committee, Senator Leahy challenged the NSA chief, General Keith Alexander: Would you agree that the 54 cases that keep getting cited by the administration were not all plots, and that of the 54 only 13 had some nexus to the US? Would you agree with that, yes or no? Alexander responded: Yes. Leahy then demanded that Alexander confirm what his deputy, Christopher Inglis, had said in the prior week's testimony: that there is only one example where collection of bulk data is what stopped a terrorist activity. Alexander responded that Inglis might have said two, not one. In fact, what Inglis had said the week before was that there was one case "that comes close to a but-for example and that's the case of Basaaly Moalin". So, who is Moalin, on whose fate the NSA places the entire burden of justifying its metadata collection program? Did his capture foil a second 9/11? A cabby from San Diego, Moalin had immigrated as a teenager from Somalia. In February, he was convicted of providing material assistance to a terrorist organization: he had transferred \$8,500 to al-Shabaab in Somalia. After the Westgate Mall attack in Nairobi, few would argue that al-Shabaab is not a terrorist organization. But al-Shabaab is involved in a local war, and is not invested in attacking the US homeland. The indictment against Moalin explicitly stated that al-Shabaab's enemies were the present Somali government and "its Ethiopian and African Union supporters". Perhaps, it makes sense for prosecutors to pursue Somali Americans for doing essentially what some Irish Americans did to help the IRA; perhaps not. But this single successful prosecution, under a vague criminal statute, which stopped a few thousand dollars from reaching one side in a local conflict in the Horn of Africa, is the sole success story for the NSA bulk domestic surveillance program.

2. There is no real evidence that the program is effective

Yochai Benkler, “Fact: The NSA Gets Negligible Intel from Americans’ Metadata. So End Collection,” GUARDIAN, 10—8—13, <http://www.theguardian.com/commentisfree/2013/oct/08/nsa-bulk-metadata-surveillance-intelligence>, accessed 10-10-13. It is hardly surprising that supporters of bulk collection fervently believe it is critical to national security. No psychologically well-balanced person could permit herself to support a program that compromises the privacy of tens of millions of Americans, costs billions of dollars, and imposes direct and articulable harm to cyber security by undermining the security of commercial products and public standards without holding such a belief truly and honestly. But the honest faith of insiders that their bureaucratic mission is true and critical is no substitute for credible evidence. A dozen years of experience has produced many public overstatements and much hype from insiders, but nothing to support the proposition that the program works at all, much less that its marginal contribution is significant enough to justify its enormous costs in money, freedom, and destabilization of internet security. No rational cost-benefit analysis could justify such a leap of faith. If the NSA cannot show real, measurable evidence of its effectiveness, evidence that doesn't collapse as soon as it is examined and isn't a vague appeal to amorphous, measurement-free "peace of mind", its bulk collection program has to go.

3. The NSAs program will only catch dumb terrorists

Leonid Bershidsky, “U.S. Surveillance Is not Aimed at Terrorists,” BLOOMBERG, 6—23—13, www.bloomberg.com/news/2013-06-23/u-s-surveillance-is-not-aimed-at-terrorists.html, accessed 10-2-13. The debate over the U.S. government's monitoring of digital communications suggests that Americans are willing to allow it as long as it is genuinely targeted at terrorists. What they fail to realize is that the surveillance systems are best suited for gathering information on law-abiding citizens. People concerned with online privacy tend to calm down when told that the government can record their calls or read their e-mail only under special circumstances and with proper court orders. The assumption is that they have nothing to worry about unless they are terrorists or correspond with the wrong people. The infrastructure set up by the National Security Agency, however, may only be good for gathering information on the stupidest, lowest-ranking of terrorists. The Prism surveillance program focuses on access to the servers of America's largest Internet companies, which support such popular services as Skype, Gmail and iCloud. These are not the services that truly dangerous elements typically use.

Surveillance Undesirable: Answers to “Terrorism”—Effectiveness Exaggerated [cont’d]**4. Claims of program effectiveness are hollow and ill-supported**

Jameer Jaffer, fellow, Open Society Foundations, “Secrecy and Freedom,” NEW YORK TIMES, Room for Debate, 6—9—13, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined>, accessed 10-4-13. Joshua, I agree with you that effectiveness matters. I can’t help but be skeptical, though. If these dragnet programs are effective, where’s the evidence? As you note, at least one of the success stories identified by anonymous intelligence officials—the story relating to Zazi—seems not to withstand scrutiny. Let’s also note that there’s no evidence the government has relied on evidence derived from these dragnet programs in criminal prosecutions. If these dragnet programs had been effective, wouldn’t we have seen at least a handful of criminal prosecutions? Of course intelligence surveillance has many purposes; gathering evidence of criminal activity is just one of them. Still, shouldn’t the apparent absence of any criminal prosecution make us question how necessary the programs really are? Lacking any more solid evidence of success, you fall back on the point that “the people who created and oversee” these programs “believe they are effective.” But unfortunately there are many reasons to question the trust you imply we should put in our national security agencies when they tell us, in essence, “we need more power to make you safe.”

Surveillance Undesirable: Answers to “Terrorism”—Info Overload

1. Our agencies end up getting overwhelmed by the sheer volume of information

Sebastian Rotella, Pulitzer Prize winning journalist, “How the NSA’s High-Tech Surveillance Helped Europeans Catch Terrorists,” PROPUBLICA, 6—19—13, www.propublica.org/article/how-the-nsas-high-tech-surveillance-helped-europeans-catch-terrorists, accessed 10-4-13.

At the same time, some European experts see the furor as a sign that the strengths of the American giant intertwine with its weaknesses. U.S. agencies devote huge resources to sophisticated technology to the detriment of analysis and human spying, they say. As a result, they say, U.S. agencies sometimes appear overwhelmed by the sheer volume of information. “The problem is not collecting information, it’s understanding it,” said Alain Bauer, a well-connected French criminologist who has served as a presidential adviser. “What is the sense of such programs? They are too big. They will not work. We are a former colonial empire. We know the value of human intelligence. It is more efficient and less expensive than technological fetishism. Fortunately, we do not have enough money to do it the other way.”

2. Building bigger haystacks will not make it easier to find the needles—can have too much information

Jameer Jaffer, fellow, Open Society Foundations, “Secrecy and Freedom,” NEW YORK TIMES, Room for Debate, 6—9—13, <http://www.nytimes.com/roomfordebate/2013/06/09/is-the-nsa-surveillance-threat-real-or-imagined>, accessed 10-4-13.

It’s also worth remembering that the intelligence community’s biggest challenge has never been collecting information; the biggest challenge has always been making sense of it. Launching new programs to collect more information can be a good way to pad the pockets of defense contractors and data-miners, but, as many have noted, it isn’t usually a good way to identify terrorist threats. The analogy is now a bit threadbare, but it’s still useful: You don’t find needles by building bigger haystacks. After the NSA launched the warrantless wiretapping program, FBI agents repeatedly complained that they were drowning in useless information. (Eric Lichtblau wrote: “The torrent of tips led [the FBI] to few potential terrorists inside the country they did not know of from other sources and diverted agents from counterterrorism work they viewed as more productive.”). One of the 9/11 Commission’s most important observations was that the intelligence community had information in the summer of 2001 that could have allowed it to prevent the 9/11 attacks. The problem wasn’t that it lacked information, but that it didn’t understand the information it had. Finally, “effectiveness” isn’t as simple as you make it out to be. A program can be effective in some very narrow sense but also seriously compromise our democracy over the long term. A program can be effective in some very narrow sense but also be fundamentally inconsistent with our values. Again, I agree that the effectiveness question is worth asking. But answering the effectiveness question isn’t as simple as asking whether these surveillance programs yielded useful information.

Surveillance Undesirable: Answers to “Terrorism”—Nuclear

1. A nuclear terrorist attack would not destroy our society or economy

John Mueller, Professor, Political Science, Ohio State University, “Think Again: Nuclear Weapons,” FOREIGN POLICY, January/February 2010, ASP.

Although former CIA chief George Tenet insists in his memoirs that one "mushroom cloud" would "destroy our economy," he never bothers to explain how the instant and tragic destruction of three square miles somewhere in the United States would lead inexorably to national economic annihilation. A nuclear explosion in, say, New York City -- as Obama so darkly invoked -- would obviously be a tremendous calamity that would roil markets and cause great economic hardship, but would it extinguish the rest of the country? Would farmers cease plowing? Would manufacturers close their assembly lines? Would all businesses, governmental structures, and community groups evaporate? Americans are highly unlikely to react to an atomic explosion, however disastrous, by immolating themselves and their economy. In 1945, Japan weathered not only two nuclear attacks but intense nationwide conventional bombing; the horrific experience did not destroy Japan as a society or even as an economy. Nor has persistent, albeit nonnuclear, terrorism in Israel caused that state to disappear -- or to abandon democracy. Even the notion that an act of nuclear terrorism would cause the American people to lose confidence in the government is belied by the traumatic experience of Sept. 11, 2001, when expressed confidence in America's leaders paradoxically soared. And it contradicts decades of disaster research that documents how socially responsible behavior increases under such conditions -- seen yet again in the response of those evacuating the World Trade Center on 9/11.

2. Terrorists cannot obtain a loose nuke and would be able to detonate it anyway

John Mueller, Professor, Political Science, Ohio State University, “Think Again: Nuclear Weapons,” FOREIGN POLICY, January/February 2010, ASP.

That's a myth. It has been soberly, and repeatedly, restated by Harvard University's Graham Allison and others that Osama bin Laden gave a group of Chechens \$30 million in cash and two tons of opium in exchange for 20 nuclear warheads. Then there is the "report" about how al Qaeda acquired a Russian-made suitcase nuclear bomb from Central Asian sources that had a serial number of 9999 and could be exploded by mobile phone. If these attention-grabbing rumors were true, one might think the terrorist group (or its supposed Chechen suppliers) would have tried to set off one of those things by now or that al Qaeda would have left some trace of the weapons behind in Afghanistan after it made its very rushed exit in 2001. Instead, nada. It turns out that getting one's hands on a working nuclear bomb is actually very difficult. In 1998, a peak year for loose nuke stories, the head of the U.S. Strategic Command made several visits to Russian military bases and pointedly reported, "I want to put to bed this concern that there are loose nukes in Russia. My observations are that the Russians are indeed very serious about security." Physicists Richard Garwin and Georges Charpak have reported, however, that this forceful firsthand testimony failed to persuade the intelligence community "perhaps because it [had] access to varied sources of information." A decade later, with no credible reports of purloined Russian weapons, it rather looks like it was the general, not the spooks, who had it right. By all reports (including Allison's), Russian nukes have become even more secure in recent years. It is scarcely rocket science to conclude that any nuke stolen in Russia is far more likely to go off in Red Square than in Times Square. The Russians seem to have had no difficulty grasping this fundamental reality. Setting off a stolen nuke might be nearly impossible anyway, outside of TV's 24 and disaster movies. Finished bombs are routinely outfitted with devices that will trigger a nonnuclear explosion to destroy the bomb if it is tampered with. And, as Stephen Younger, former head of nuclear weapons research and development at Los Alamos National Laboratory, stresses, only a few people in the world know how to cause an unauthorized detonation of a nuclear weapon. Even weapons designers and maintenance personnel do not know the multiple steps necessary. In addition, some countries, including Pakistan, store their weapons disassembled, with the pieces in separate secure vaults.

Surveillance Undesirable: Answers to “Terrorism”—Nuclear [cont’d]

3. There is little evidence that Al Qaeda is currently pursuing nuclear weapons

John Mueller, Professor, Political Science, Ohio State University, “Think Again: Nuclear Weapons,” FOREIGN POLICY, January/February 2010, ASP.

Al Qaeda may have had some interest in atomic weapons and other weapons of mass destruction (WMD). For instance, a man who defected from al Qaeda after he was caught stealing \$110,000 from the organization -- “a lovable rogue,” “fixated on money,” who “likes to please,” as one FBI debriefer described Jamal al-Fadl -- has testified that members tried to purchase uranium in the mid-1990s, though they were scammed and purchased bogus material. There are also reports that bin Laden had “academic” discussions about WMD in 2001 with Pakistani nuclear scientists who did not actually know how to build a bomb. But the Afghanistan invasion seems to have cut any schemes off at the knees. As analyst Anne Stenersen notes, evidence from an al Qaeda computer left behind in Afghanistan when the group beat a hasty retreat indicates that only some \$2,000 to \$4,000 was earmarked for WMD research, and that was mainly for very crude work on chemical weapons. For comparison, she points out that the Japanese millennial terrorist group, Aum Shinrikyo, appears to have invested \$30 million in its sarin gas manufacturing program. Milton Leitenberg of the Center for International and Security Studies at the University of Maryland-College Park quotes Ayman al-Zawahiri as saying that the project was “wasted time and effort.” Even former International Atomic Energy Agency inspector David Albright, who is more impressed with the evidence found in Afghanistan, concludes that any al Qaeda atomic efforts were “seriously disrupted” -- indeed, “nipped in the bud” -- by the 2001 invasion of Afghanistan and that after the invasion the “chance of al Qaeda detonating a nuclear explosive appears on reflection to be low.”

4. It remains very difficult for a group to manufacture its own nuclear weapons

John Mueller, Professor, Political Science, Ohio State University, “Think Again: Nuclear Weapons,” FOREIGN POLICY, January/February 2010, ASP.

An editorialist in *Nature*, the esteemed scientific journal, did apply that characterization to the manufacture of uranium bombs, as opposed to plutonium bombs, last January, but even that seems an absurd exaggeration. Younger, the former Los Alamos research director, has expressed his amazement at how “self-declared ‘nuclear weapons experts,’ many of whom have never seen a real nuclear weapon,” continue to “hold forth on how easy it is to make a functioning nuclear explosive.” Uranium is “exceptionally difficult to machine,” he points out, and “plutonium is one of the most complex metals ever discovered, a material whose basic properties are sensitive to exactly how it is processed.” Special technology is required, and even the simplest weapons require precise tolerances. Information on the general idea for building a bomb is available online, but none of it, Younger says, is detailed enough to “enable the confident assembly of a real nuclear explosive.” A failure to appreciate the costs and difficulties of a nuclear program has led to massive overestimations of the ability to fabricate nuclear weapons. As the 2005 Silberman-Robb commission, set up to investigate the intelligence failures that led to the Iraq war, pointed out, it is “a fundamental analytical error” to equate “procurement activity with weapons system capability.” That is, “simply because a state can buy the parts does not mean it can put them together and make them work.” For example, after three decades of labor and well over \$100 million in expenditures, Libya was unable to make any progress whatsoever toward an atomic bomb. Indeed, much of the country’s nuclear material, surrendered after it abandoned its program, was still in the original boxes.

5. Nuclear terror risk is exaggerated--hard to build, hard to steal, hard to smuggle into the U.S.

Francis Gavin, Tom Slick Professor of International Affairs, University of Texas at Austin, “Same As It Ever Was: Nuclear Alarmism, Proliferation, and the Cold War,” INTERNATIONAL SECURITY v. 34 n. 3, Winter 2009/2010, p. 19-20.

Experts disagree on whether nonstate actors have the scientific, engineering, financial, natural resource, security, and logistical capacities to build a nuclear bomb from scratch. According to terrorism expert Robin Frost, the danger of a “nuclear black market” and loose nukes from Russia may be overstated. Even if a terrorist group did acquire a nuclear weapon, delivering and detonating it against a U.S. target would present tremendous technical and logistical difficulties. Finally, the feared nexus between terrorists and rogue regimes may be exaggerated. As nuclear proliferation expert Joseph Cirincione argues, states such as Iran and North Korea are “not the most likely sources for terrorists since their stockpiles, if any, are small and exceedingly precious, and hence well-guarded.” Chubin states that there “is no reason to believe that Iran today, any more than Sadaam Hussein earlier, would transfer WMD [weapons of mass destruction] technology to terrorist groups like al-Qaida or Hezbollah.”

Surveillance Undesirable: Answers to “Terrorism”—Nuclear [cont’d]

6. Worst case nuclear terror unlikely--they incorrectly assume infallible, indestructible terrorists

Francis Gavin, Tom Slick Professor of International Affairs, University of Texas at Austin, "Same As It Ever Was: Nuclear Alarmism, Proliferation, and the Cold War," *INTERNATIONAL SECURITY* v. 34 n. 3, Winter 2009/2010, p. 20.

Even if a terrorist group were to acquire a nuclear device, expert Michael Levi demonstrates that effective planning can prevent catastrophe: for nuclear terrorists, what “can go wrong might go wrong, and when it comes to nuclear terrorism, a broader, integrated defense, just like controls at the source of weapons and materials, can multiply, intensify, and compound the possibilities of terrorist failure, possibly driving terrorist groups to reject nuclear terrorism altogether.” Warning of the danger of a terrorist acquiring a nuclear weapon, most analyses are based on the inaccurate image of an “infallible ten-foot-tall enemy.” This type of alarmism, writes Levi, impedes the development of thoughtful strategies that could deter, prevent, or mitigate a terrorist attack: “Worst-case estimates have their place, but the possible failure-averse, conservative, resource-limited-five-foot-tall nuclear terrorist, who is subject not only to the laws of physics but also to Murphy’s law of nuclear terrorism, needs to become just as central to our evaluations of strategies.”

7. Claims that Al Qaeda wants nuclear weapons are overstated

Francis Gavin, Tom Slick Professor of International Affairs, University of Texas at Austin, "Same As It Ever Was: Nuclear Alarmism, Proliferation, and the Cold War," *INTERNATIONAL SECURITY* v. 34 n. 3, Winter 2009/2010, p. 20-21.

A recent study contends that al-Qaida’s interest in acquiring and using nuclear weapons may be overstated. Anne Stenersen, a terrorism expert, claims that “looking at statements and activities at various levels within the al-Qaida network, it becomes clear that the network’s interest in using unconventional means is in fact much lower than commonly thought.” She further states that “CBRN [chemical, biological, radiological, and nuclear] weapons do not play a central part in al-Qaida’s strategy.” In the 1990s, members of al-Qaida debated whether to obtain a nuclear device. Those in favor sought the weapons primarily to deter a U.S. attack on al-Qaida’s bases in Afghanistan. This assessment reveals an organization at odds with that laid out by nuclear alarmists of terrorists obsessed with using nuclear weapons against the United States regardless of the consequences. Stenersen asserts, “Although there have been various reports stating that al-Qaida attempted to buy nuclear material in the nineties, and possibly recruited skilled scientists, it appears that al-Qaida central have not dedicated a lot of time or effort to developing a high-end CBRN capability. . . . Al-Qaida central never had a coherent strategy to obtain CBRN: instead, its members were divided on the issue, and there was an awareness that militarily effective weapons were extremely difficult to obtain.” 57 Most terrorist groups “assess nuclear terrorism through the lens of their political goals and may judge that it does not advance their interests.” As Frost has written, “The risk of nuclear terrorism, especially true nuclear terrorism employing bombs powered by nuclear fission, is overstated, and that popular wisdom on the topic is significantly flawed.”